Dr.WEB

Enterprise Security Suite

Installation Manual

This document is for information and reference purposes in relation to the specified software of the Dr.Web family. This document is not a ground for exhaustive conclusions about the presence or absence of any functional and/or technical features in the software of the Dr.Web family and cannot be used to determine whether the software of the Dr.Web family matches any requirements, technical task and/or parameters, and other third-party documents.

Trademarks

Disclaimer

In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web Enterprise Security Suite
Version 11.0.2
Installation Manual
7/2/2020

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125040

Website: https://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Chapter 1: Dr.Web Enterprise Security Suite

1.1. Introduction

1.1.1. About Manual

Documentation of Dr.Web Enterprise Security Suite anti-virus network administrator is intended to introduce general features and provide detailed information on the organisation of the complex anti-virus protection of corporate computers using Dr.Web Enterprise Security Suite.

Documentation of the anti-virus network administrator contains the following parts:

1. **Installation Manual** (the **drweb-11.0-esuite-install-manual-en.pdf** file)

   Installation Manual will be useful to the organisation manager who makes the decision to purchase and install a system of comprehensive anti-virus protection.

   Installation Manual explains how to build an anti-virus network and install its general components.

2. **Administrator Manual** (the **drweb-11.0-esuite-admin-manual-en.pdf** file)

   Administrator Manual is meant for *anti-virus network administrator*—the employee of organisation who is responsible for the anti-virus protection of computers (workstations and servers) of this network.

   Anti-virus network administrator should either have a system administrator privileges or work closely with a local network administrator, be competent in anti-virus protection strategy and know in detailes Dr.Web anti-virus packages for all operating systems that are used in the network.

3. **Appendices** (the **drweb-11.0-esuite-appendices-en.pdf** file)

   Appendices provide technical information, describes the configuration parameters of the Anti-virus modules and explains the syntax and values of instructions used for operation with them.

   > Documentation contains cross-references between mentioned documents. If you download these documents to the local computer, cross-references work only if documents are located in the same folder and have their initial names.

Also, the following Manuals are provided:

1. **Anti-virus Network Quick Installation Guide**

   Contains brief information on installation and initial configuration of anti-virus network components. For detailed information refer to administrator documentation.

2. **Manuals on managing stations**

   Contain the information about centralized configuration of anti-virus software of workstations which is provided by anti-virus network administrator via the Dr.Web Security Control Center.

3. **User Manuals**

   Contain the information about configuration of Dr.Web anti-virus software provided on protected stations directly.

All the listed Manuals are provided also within Dr.Web Enterprise Security Suite product and can be opened via Dr.Web Security Control Center.

Before reading these documents, make sure you have the latest version of the corresponding Manuals for your product version. The Manuals are constantly updated and the current version can always be found at the official web site of Doctor Web at https://download.drweb.com/doc/.

1.1.2. Conventions and Abbreviations

Conventions

The following symbols and text conventions are used in this guide:

Convention	Comment
(!)	Important note or instruction.
⚠	Warning about possible errors or important notes to which you should pay special attention.
Anti-virus network	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references on the document chapters or internal hyperlinks to web pages.

Abbreviations

The following abbreviations can be used in the Manual without further interpretation:

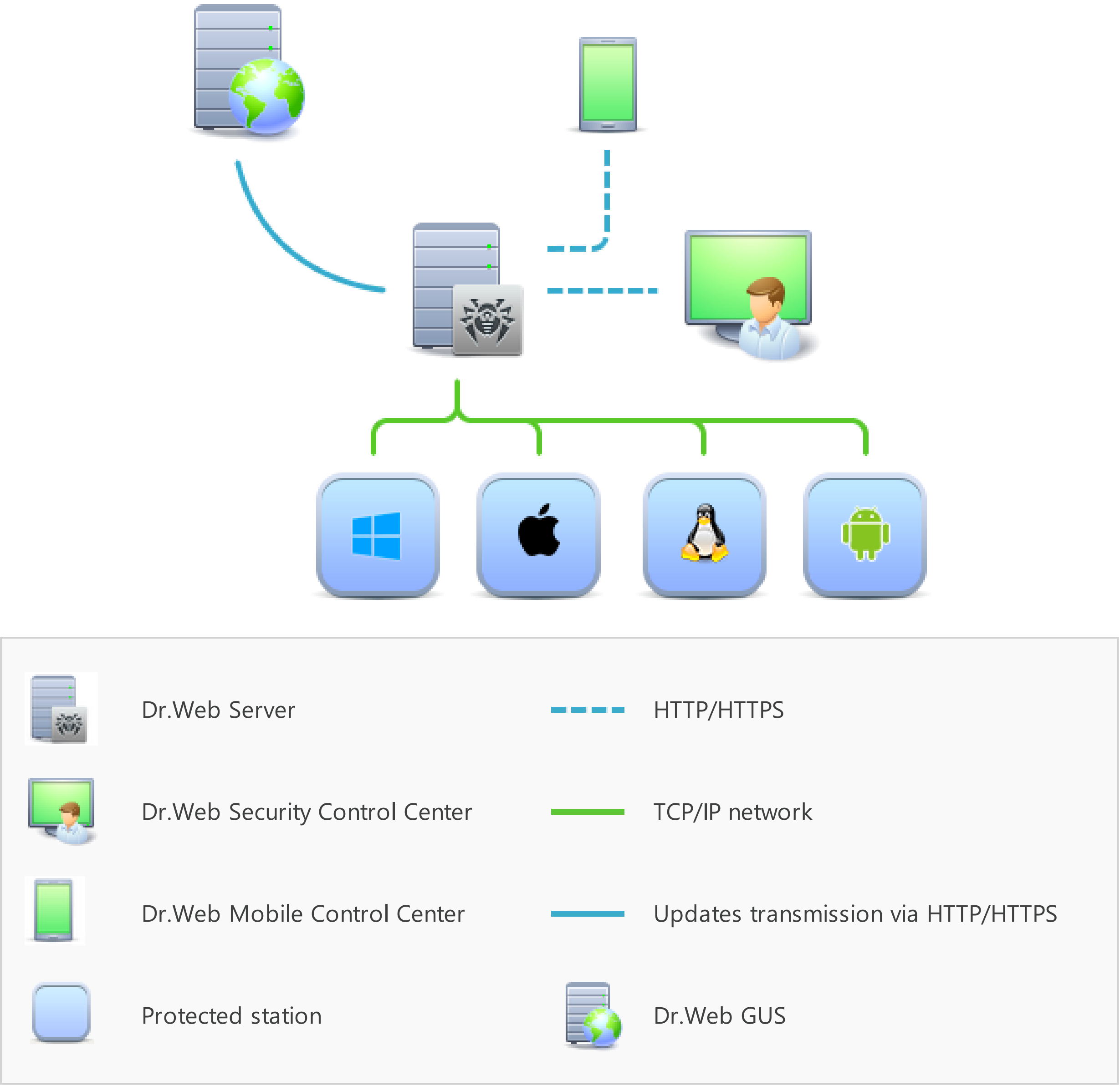
- ACL—Access Control List,
- CDN—Content Delivery Anti-virus network,
- DB, DBMS—Database, Database Management System,
- DFS—Distributed File System,
- DNS—Domain Name System,
- Dr.Web GUS—Dr.Web Global Update System,
- FQDN—Fully Qualified Domain Name,
- GUI—Graphical User Interface, a GUI version of a program—a version using a GUI,
- LAN—Local Area Network,
- MTU—Maximum Transmission Unit,
- NAP—Network Access Protection,
- OS—Operating System,
- TTL—Time To Live,

- UDS—UNIX domain socket.

1.2. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of integrated and secure complex anti-virus protection either local company network including mobile devices, or home computers of employers.

An aggregate of computers and mobile devices on which Dr.Web Enterprise Security Suite cooperating components are installed, represents a single *anti-virus network*.


Dr.Web Server
HTTP/HTTPS
Dr.Web Security Control Center
TCP/IP network
Dr.Web Mobile Control Center
Updates transmission via HTTP/HTTPS
Protected station
Dr.Web GUS

Picture 1-1. The logical structure of the anti-virus network

Dr.Web Enterprise Security Suite anti-virus network has a *client-server* architecture. Its components are installed on a computers and mobile devices of users and administrators as well as on a computers that function as LAN servers. Anti-virus network components exchange information via TCP/IP network protocols. Anti-virus software can be installed (and manage them afterwards) on protected stations either via the LAN, or via the Internet.

Central Protection Server

Central protection Server is installed on a computer of anti-virus network, and installation can be performed on any computer, not only on that functioning as a LAN server. General requirements to this computer are given in the System Requirements section.

Cross-platform Server software allows to use a computer under the following operating systems as a Server:

- Windows® OS,
- UNIX® system-based OS (Linux®, FreeBSD®).

Central protection Server stores distribution kits of anti-virus packages for different OS of protected computers, updates of virus databases and anti-virus packages, license keys and package settings of protected computers. Server receives updates of anti-virus protection components and virus databases via the Internet from the Global Update System and propagate updates on protected stations.

Hierarchical structure of several Servers can be established to serve protected stations of anti-virus network.

Server supports the backup of critical data (databases, configuration files, etc.).

Server writes single log of anti-virus network events.

Single Database

The single database is connected to the central protection Server and stores statistic data on anti-virus network events, settings of the Server itself, parameters of protected stations and anti-virus components, installed on protected stations.

You can use the following types of databases:

Embedded database. The SQLite3 database that is embedded into the central protection Server directly is provided.

External database. Inbuilt drivers for connecting the following databases are provided:

- MySQL,
- Oracle,
- PostgreSQL,
- ODBC driver to connect other databases such as Microsoft SQL Server/Microsoft SQL Server Express.

You can use any database that corresponds to your demands. Your choice should be based on the needs that must be satisfied by the data store, such as: capability to service the anti-virus network of corresponding size, features of database software maintenance, administration capabilities provided by the database itself and also requirements and standards which are accepted for use in your company.

Central Protection Control Center

Central protection Control Center is automatically installed with the Server and provides the web interface for remote managing of the Server and the anti-virus network by means of editing the settings of the Server and protected computers settings stored on the Server and protected computers.

The Control Center can be opened on any computer that have the network access to the Server. The Control Center can be used almost under any operating system with full use on the following web browsers:

- Windows® Internet Explorer®,
- Microsoft Edge®,
- Mozilla® Firefox®,
- Google Chrome®.

The list of possible variants of use is given in the System Requirements section.

Central protection Control Center provides the following features:

- Serviceability of Anti-virus installation on protected stations including: remote installation on protected stations under Windows OS with preliminary browsing the network to search computers; Creation of distribution files with unique identifiers and parameters of connection to the Server to facilitate Anti-virus installation process by the administrator or possibility of Anti-virus installation by users on stations by oneself (detailed information see in the Installing Dr.Web Agent section).
- Facilitate administering based on grouping of anti-virus network workstations.
- Feasibility of centralized administrating of stations anti-virus packages including: uninstallation either separate components or entire Anti-virus on stations under Windows OS; configuring parameters of anti-virus package components; assigning permissions to set up and administer the anti-virus packages on protected computers for users of these computers.
- Centralized administering of workstations anti-virus check including: remote launch of anti-virus check either according the specified schedule or direct request from administrator for the Control Center; centralized configuration of check parameters and transmitting them to the workstations to launch the local check with these parameters.
- Receiving the statistic information on protected stations states, viral statistics, installed anti-virus software state, running anti-virus components state and also, the list of hardware and software on protected station.
- Flexible administrating system of Server and anti-virus network based on opportunity of permissions delimiting for different administrators and also, possibility to connect administrators via the external authorization systems such as Active Directory, LDAP, RADIUS, PAM.
- Managing the licensing of workstations anti-virus protection with branched system of assigning licenses to stations, groups of stations and also, granting licenses between several Servers in multiserver configuration of anti-virus network.

- Wide set of setting to configure the Server and its separate components including: configuring schedule to maintain the Server; plug in user hooks; flexible configuration of update system of all anti-virus network components from the GUS and further propagation of updates on stations; configuring the system of administrator notifications about anti-virus network events with different methods of notification delivering; configuring neighbor connections to configure multiserver anti-virus network.

Detailed information on described functions is given in the **Administrator Manual**.

The par of the Control Center is the Web server that is automatically installed with the Server. The general task of the Web server is performing operation with web pages of the Control Center and clients network connections.

Central Protection Mobile Control Center

As a separate component, the Mobile Control Center is provided. It is designed for installation and operation on mobile devices under iOS® and Android™ OS. General requirements to the application are given in the System Requirements section.

Mobile Control Center connects to the Server according to the anti-virus network administrator credentials including via an encrypted protocol. Mobile Control Center supports the base set of Control Center functions:

1. Manage Dr.Web Server repository:
   - view the products state in the repository;
   - launch repository update from Dr.Web Global Update System.
2. Manage stations on which an update of anti-virus software is failed:
   - display failed stations;
   - update components on failed stations.
3. Display statistics information on anti-virus network state:
   - number of stations registered at Dr.Web Server and their current state (online/offline);
   - viral statistics for protected stations.
4. Manage new stations waiting for connection to Dr.Web Server:
   - approve access;
   - reject stations.
5. Manage anti-virus components installed on anti-virus network stations:
   - launch the fast or full scan either for selected stations or for all stations of selected groups;
   - setup Dr.Web Scanner reaction on malware detection;
   - view and manage files in the Quarantine either for selected stations or for all stations in the selected group.

6. Manage stations and groups:
   - view properties;
   - view and manage components composition of anti-virus package;
   - delete;
   - send custom messages to stations;
   - reboot stations under Windows OS;
   - add to favorites list for the quick assess.
7. Search for stations and groups in an anti-virus network by different parameters: name, address, ID.
8. View and manage messages on major events in an anti-virus network via the interactive Push notifications:
   - display all notifications at Dr.Web Server;
   - set reactions on notification events;
   - search notification by specified filter parameters;
   - delete notifications;
   - exclude notifications from automatic deletion.

You can download Mobile Control Center from the Control Center or directly in App Store and Google Play.

Network Stations Protection

On protected computers and mobile devices of the network, the control module (Agent) and the anti-virus package for corresponding operating system are installed.

Cross-platform software allows to provide anti-virus protection of computers and mobile devices under the following operating systems:

- Windows® OS,
- UNIX® system-based OS,
- macOS®,
- Android OS.

Either user computers or LAN servers can be protected stations. Particularly, anti-virus protection of the Microsoft® Outlook® mail system is supported.

Control module performs regular updates of anti-virus components and virus databases from the Server and also, sends information on virus evens on protected computer to the Server.

If the central protection Server is not accessible, it is possible to update virus databases on protected stations via the Internet from the Global Update System.

Depending on the operating system of the station, the following protection functions are provided:

Stations under Windows® OS

Anti-virus check

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the Control Center including rootkits check is supported.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Mail monitor

Checks all incoming and outgoing mail messages when using the mail clients.

The spam filter is is also available (if the license permits this function).

Web monitor

Checks all calls to web sites via the HTTP protocol. Neutralises malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Office Control

Controls access to network and local resources, in particular, limits access to web sites. Allows to control the integrity of important files from the accidental change or virus infecting and limit the access to unwanted information for employees.

Firewall

Protects computers from external unauthorised access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Self-protection

Protects files and folders of Dr.Web Enterprise Security Suite from unauthorised or accidental removal and modification by user or malicious software. If self-protection is enabled, access to files and folders of Dr.Web Enterprise Security Suite is granted to Dr.Web processes only.

Preventive protection

Prevents of potential security threats. Controls the access to the operating system critical objects, controls drivers loading, programs autorun and system services operation and also monitors running processes and blocks them in case of detection of viral activity.

Stations under UNIX® system-based OS

Anti-virus check

Scanning engine. Provides the anti-virus scanning service (contents of files and disk boot records and other data received from other components of Dr.Web for UNIX). It queues files that are waiting to be scanned. Cures the files that can be cured.

Anti-virus check, Quarantine management

The component which scans file system objects and manages quarantined files. It receives scanning tasks from other Dr.Web for UNIX components. Checks file system directories according to a received task, transmits files for scanning to the scanning engine. It also removes infected files, moves them to quarantine, restores them from quarantine, and manages quarantine directories. The component creates and updates cache that stores information on scanned files to lessen the frequency of repeated file scanning.

Used by components that scan file system objects, such as SpIDer Guard (for Linux, SMB, NSS).

Web traffic check

ICAP server analyzing requests and traffic which goes via HTTP proxy servers. It also prevents transmitting infected files and access to the network hosts belonging to the Internet resources categories and to black lists, created by the system administrator.

File monitor for GNU/Linux system-based OS

The Linux file system monitor. It operates in a resident mode and monitors file operations (creation, opening, closing, and running of a file) in the GNU/Linux file systems. It sends to the files check component tasks to scan new and modified files or executable files upon a program startup.

File monitor for Samba directories

Monitor of Samba shared file system directories. It operates as a resident mode and monitors file operations (creation, opening, closing, and read or write operations) in directories used by SMB file server Samba. It sends to the files check component contents of new and modified files for the check.

NSS file monitor

NSS volumes monitor (Novell Storage Services). It operates as a resident mode and monitors file operations (creation, opening, closing and write operations) on NSS volumes mounted in the specified file system point. It sends to the files check component contents of new and modified files for the check.

Internet connections check

The component for monitoring network traffic and URLs. It is designed to check data downloaded from the network to the local host and transmitted from it to the external network for threats. The components also prevents connections with the network hosts, included not only to the unwanted categories of web resources, but also to black lists created by the system administrator.

Mail monitor

The component for scanning of emails. Analyzes the messages of email protocols, sorts out emails and prepares them for scanning for threats. It can operate in two modes:

1. A filter for mail servers(Sendmail, Postfix, etc.) connected via the interface Milter, Spamd or Rspamd.
2. A transparent proxy of mail protocols (SMTP, POP3, IMAP). In this mode, it uses SpIDer Gate.

Stations under macOS®

Anti-virus check

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the Control Center is supported.

File monitor

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

Web monitor

Checks all calls to web sites via the HTTP protocol. Neutralises malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Mobile devices under Android OS

Anti-virus check

Scans a mobile device on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the Control Center is supported.

File monitor

The constant file system protection in the real-time mode. The check of all files as they are saved in the memory of the device.

Calls and SMS Filter

Filtering the incoming phone calls and SMS allows to block the undesired messages and calls, such as advertisements or messages and calls from unknown numbers.

Anti-theft

Detect the device location or lock its functions in case it has been lost or stolen.

Restricting Internet Access

URL filter allows to protect user of the mobile device from unsolicited Internet sites.

Firewall

Protects the mobile device from external unauthorised access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Security Troubleshooting

Diagnostic and analysis of the security of mobile device and resolving the detected problems and vulnerabilities.

Application launch control

Blocks the launch on mobile device those applications that are not included into the list of allowed by administrator.

Providing a Connection between Anti-virus Network Components

To provide stable and secure connection between anti-virus network components, the following features are presented:

Dr.Web Proxy server

Proxy server can be optionally included in an anti-virus network. The main function of the Proxy server is to provide connection between the Server and protected stations in case if direct connection is impossible.

The Proxy server allows using any computer included in an anti-virus network for the following purposes:

- As update relay center to reduce the network load on the Server and on connection between the Server and the Proxy server, as well as to reduce the time required for protected stations to get updates by using the caching function.
- As a distribution center of virus events coming from protected stations to the Server, which also reduces network load and allows keeping up with cases when, for example, a group of stations is located in a network segment, which is isolated from the segment the Server is in.

Traffic compression

Special compression algorithms are applicable for transferring data between the anti-virus network components to reduced network traffic to minimum.

Traffic encryption

Data transferred between the anti-virus network components can be encrypted to provide additional secure level.

Additional Features

NAP Validator

NAP Validator is provided as a separate component and allows to use Microsoft Network Access Protection (NAP) technology to check health of protected stations software. The resulting security is achieved through the implementation of the requirements for performance of network stations.

Repository loader

Dr.Web Repository loader is provided as a separate utility and allows to download products of Dr.Web Enterprise Security Suite from the Global Update System. It can be used for downloading of Dr.Web Enterprise Security Suite products updates to place them on the Server not connected to the Internet.

1.3. System Requirements

For Dr.Web Enterprise Security Suite to be installed and function the following is required:

- Anti-virus network computers should have access to Dr.Web Server or to the Proxy server.
- For interaction between the anti-virus components, the following ports must be opened on used computers:

Port numbers	Protocols	Connection directions	Purpose
2193	TCP	• incoming, outgoing for the Server and Proxy server • outgoing for the Agent	For connection between the Server and anti-virus components and for interserver communications. Also is used by Proxy server to establish a connection with clients.
	UDP	incoming, outgoing	For the Network Scanner.
139, 445	TCP	• incoming for the Server • incoming, outgoing for the Agent • outgoing for the computer on which the Control Center is opened	For the Network Installer.
	UDP	incoming, outgoing	

Port numbers	Protocols	Connection directions	Purpose
9080	HTTP	• incoming for the Server • outgoing for the computer on which the Control Center is opened	For Dr.Web Security Control Center.
9081	HTTPS		
10101	TCP		For Server remote diagnostic utility.
80	HTTP	outgoing	For receiving updates from GUS.
443	HTTPS		

Dr.Web Server requires:

Component	Requirement
CPU	CPU that supports SSE2 instructions and has 1,3 GHz or faster clock frequency.
RAM	• Minimal requirements: 1 GB. • Recommended requirements: 2 GB and more.
Free disk space	Up to 12 GB: up to 8 GB for a embedded database (installation catalog) and up to 4GB for the system temporary catalog (for work files). Depending on the Server settings, additional space may be required to store temporary files, e.g. to store personal installation packages of Agents (app. 17 MB for each) in the `var\installers-cache` subfolder of Dr.Web Server installation folder. ⚠ To install the Server, it is required on Windows OS system disk or in the `/var/tmp` for UNIX system-based OS (or in the other temporary files folder, if it is redefined), not dependently on the Server installation folder, at least 4,3 GB for the general distribution kit and 2,5 GB for the extra distribution kit of free system disk space to launch the installer and unpack temporary files.
Operating system	• Windows; • Linux; • FreeBSD. Complete list of supported OS see in the **Appendices** document, in Appendix A.
Supported virtual and cloud environments	Can be used under operating systems meeting the above-mentioned requirements, in virtual and cloud environments, including: • VMware; • Hyper-V; • Xen;

Component	Requirement
	• KVM.
Other	For the installation of Dr.Web Server for UNIX system-based OS, the following libraries are required: `lsb` v. `3` or later, `glibc` v. `2.7` and later. To use **Oracle** DB, the `Linux kernel AIO access library` (`libaio`) is required.

Additional utilities supplied with Dr.Web Server (are available for downloading via the Control Center, in the **Administration** → **Utilities** section) must be launched on a computer that meets the system requirements for Dr.Web Server.

Dr.Web Proxy Server requires:

Component	Requirement
CPU	CPU that supports SSE2 instructions and has 1,3 GHz or faster clock frequency.
RAM	Not less than 1 GB.
Free disk space	Not less than 1 GB.
Operating system	• Windows; • Linux; • FreeBSD. Complete list of supported OS see in the **Appendices** document, in Appendix A.
Other	For the installation of Proxy Server for UNIX system-based OS: `lsb` v. `3` or later.

Dr.Web Security Control Center requires:

a) Web browser:

Web browser	Support
Windows Internet Explorer 11	Supported.
Microsoft Edge 0.10 and later	
Mozilla Firefox 25 and later	
Google Chrome 30 and later	
Opera® 10 and later	Allowed to be used, but operating is not guaranteed.

Web browser	Support
Safari® 4 and later	

For the Windows Internet Explorer web browser, please note the following features:

- Full operability of the Control Center under web browser with the **Enhanced Security Configuration for Windows Internet Explorer** mode enabled is not guaranteed.
- If you install Server on a computer with a '_' (underline) character in the name, configuration of Server with Dr.Web Security Control Center by use of Windows Internet Explorer will not be available. In this case, use other web browser.
- For proper operation of the Control Center, IP address and/or DNS name of computer with installed Dr.Web Server must be added to the trusted sites of a web browser, on which you open Control Center.
- For proper opening of Control Center via the **Start** menu under Windows 8 and Windows Server 2012 OS with tiled interface, set the following parameters of a web browser: **Tools** → **Programs** → **Opening Internet Explorer** set the **Always in Internet Explorer** flag.
- For proper operation with the Control Center via the Windows Internet Explorer web browser using the secure `https` protocol, you must install all the latest updates to the web browser.
- Operation with the Control Center via the Windows Internet Explorer web browser in the compatibility mode is not supported.

b) Recommended screen resolution to use Dr.Web Security Control Center is 1280x1024 pt.

Dr.Web Mobile Control Center requires:

Requirements are differ depending on the operating system on which the application is installed:

Operating system	Requirement	
	Operating system version	Device
iOS	iOS 8 and later	Apple® iPhone® Apple® iPad®
Android	Android 4.0 and later	–

The NAP requires:

For the Server

- Windows Server® 2008 OS.

For the Agents

- Windows XP SP3 OS, Windows Vista OS, Windows Server 2008 OS.

Dr.Web Agent and the full anti-virus package require:

Requirements are differ depending on the operating system on which anti-virus solution is installed (the full list of supported OS see in the **Appendices** document, in Appendix A. The Complete List of Supported OS Versions):

- Windows OS:

Component	Requirement
CPU	1 GHz CPU or faster.
Free RAM	Not less than 512 MB.
Free disk space	1 GB for executable files + extra disk space for logs and temporary files.
Other	1. **Dr.Web Agent for Windows** context help requires Windows® Internet Explorer® 6.0 or later. 2. For Dr.Web for Outlook extension the Microsoft Outlook client from the Microsoft Office package is required: • Outlook 2000; • Outlook 2002; • Outlook 2003; • Outlook 2007; • Outlook 2010 SP2; • Outlook 2013; • Outlook 2016.

- Linux system-based OS:

Component	Requirement
CPU	CPU with the following Intel/AMD architecture and command system are supported: 32-bit (IA-32, x86); 64-bit (x86-64, x64, amd64).
Free RAM	Not less than 512 MB.
Free disk space	Not less than 400 MB of free disk space on a volume on which Anti-virus folders are placed.

- macOS, Android OS: configuration requirements coincide with the requirements for operating system.

Dr.Web Agent can be used under operating systems meeting the above-mentioned requirements, in virtual and cloud environments, including:

- VMware;
- Hyper-V;
- Xen;
- KVM.

> No other anti-virus software (including other versions of Dr.Web anti-virus programs) should be installed on the workstations of an anti-virus network managed by Dr.Web Enterprise Security Suite.

> Functionality of Agents is described in the user manuals for corresponding OS.

1.4. Distribution Kit

The program software is distributed depending on the OS of the selected Dr.Web Server:

1. For UNIX system-base OS:
   - `drweb-11.00.2-`*<build>*`-esuite-server-`*<OS_version>*`.tar.gz.run`

     Dr.Web Server general distribution kit
   - `drweb-11.00.2-`*<build>*`-esuite-extra-`*<OS_version>*`.tar.gz.run`

     Dr.Web Server extra distribution kit
   - `drweb-11.00.2-`*<build>*`-esuite-proxy-`*<OS_version>*`.tar.gz.run`

     Dr.Web Proxy Server
   - `drweb-reploader-`*<OS>*`-`*<bitness>*

     Console version of Dr.Web Repository Loader
2. For Windows OS:
   - `drweb-11.00.2-`*<build>*`-esuite-server-`*<OS_version>*`.exe`

     Dr.Web Server general distribution kit
   - `drweb-11.00.2-`*<build>*`-esuite-extra-`*<OS_version>*`.exe`

     Dr.Web Server extra distribution kit
   - `drweb-11.00.2-`*<build>*`-esuite-proxy-`*<OS_version>*`.exe`

     Dr.Web Proxy Server
   - `drweb-11.05.4-`*<build>*`-esuite-agent-activedirectory.msi`

     Dr.Web Agent for Active Directory

- `drweb-11.00.1-<`*build*`>-esuite-modify-ad-schema-<`*OS_version*`>.exe`

  Utility for Active Directory scheme modification

- `drweb-11.00.1-<`*build*`>-esuite-aduac-<`*OS_version*`>.msi`

  Utility to change attributes for Active Directory objects

- `drweb-11.00.1-<`*build*`>-esuite-napshv-<`*OS_version*`>.msi`

  NAP Validator

- `drweb-11.05.2-<`*build*`>-esuite-agent-full-windows.exe`

  Dr.Web Agent full installer. Also included into the extra distribution kit of Dr.Web Server.

- `drweb-reploader-windows-<`*bitness*`>.exe`

  Console version of Dr.Web Repository Loader

- `drweb-reploader-gui-windows-<`*bitness*`>.exe`

  GUI version of Dr.Web Repository Loader

Dr.Web Server distribution kit contains two packages:

1. *General distribution kit*—basic distribution kit to install Dr.Web Server. Composition is similar to composition of previous versions of Dr.Web Enterprise Security Suite distribution.

   General distribution kit performs the installation of Dr.Web Server itself and includes anti-virus protection packages for stations under Windows OS only.

2. *Extra distribution kit*—includes distributions of all products, which are provided for installation on protected stations under all supported OS.

   The package is installed as an additional on a computer with Dr.Web Server *general distribution kit* installed.

   ⚠ Extra distribution kit must be installed from the same type of package as a general distribution kit.

Dr.Web Server general distribution kit contains the following components:

- Dr.Web Server software for the respective OS,
- Dr.Web Agents software and anti-virus packages software for staions under Windows OS,
- Dr.Web Security Control Center software,
- Virus databases,
- Dr.Web Security Control Center extension,
- Dr.Web Server FrontDoor extension,
- Manuals, templates, and examples.

In addition to the distribution kit, serial numbers are also supplied. Having registered these serial numbers one can get files with a Server key and an Agent key.

Chapter 2: Licensing

The license is required for the operation of Dr.Web Enterprise Security Suite anti-virus solution.

Dr.Web Enterprise Security Suite license compound and price depend on the number of protected stations including the servers within Dr.Web Enterprise Security Suite network in a position of protected stations.

> Before purchasing a license for a Dr.Web Enterprise Security Suite solution you should carefully consider this information and discuss all the details with your local distributor. The number of Dr.Web Servers running the network does not affect the license price.

License Key File

Rights to use Dr.Web Enterprise Security Suite are regulated by license key files.

> A license key file is write-protected by the mechanism of electronic signature. Editing a file makes it invalid. To avoid occasionally corrupting of a license key file, you must not modify and/or save it after opening in a text editor.

License key files come in a zip-archive, which contains one or several key files for protected stations.

The user can receive the key files by one of the following ways:

- A license key file is included into Dr.Web Enterprise Security Suite anti-virus distribution kit at a purchasing, if license files were included at kitting. However, generally only serial numbers are provided.
- A license key file is sent to users by email after the product serial number has been registered at Doctor web company web site at https://products.drweb.com/register/ unless other address specified in the registration card attached to the product. Visit the web site above, fill the form with the buyer information and in the corresponding field, type the registration serial number (it is written on the registration card). An archive with key files will be sent to the designated email address. Also, you will be allowed to download the key files directly from the web site.
- A license key file can be provided on a separate carrier.

It is recommended to keep a license key file until its expiration and use it during the reinstallation and restoring the program components. In case a license key file is lost, you can repeat the registration on the web site specified above and restore the license key file. Note that you will need to enter the same registration serial number and the same buyer information as during the first registration, you can change the email address only. In this case, a license key file will be sent to the new address.

To familiarize yourself with the anti-virus, you can use demo key files. Such key files provide the full functionality of the main anti-virus components but have a limited term of use. Demo key files are sent upon request made through the web form at https://download.drweb.com/demoreq/biz/. Your request will be examined individually. In case of approval, an archive with license key files will be sent to the designated email address.

The use of key files during the installation is described in p. Installing Dr.Web Server.

The use of key files for already deployed anti-virus network is described in **Administration Manual**, p. License Manager.

Chapter 3: Getting Started

3.1. Creating Anti-virus Network

Quick start to an anti-virus network deployment:

1. Make a plan of the anti-virus network structure, include all protected computers and mobile devices.

   Select a computer to perform the functions of Dr.Web Server. The anti-virus network can incorporate several Dr.Web Servers. The features of such configuration are described in **Administrator Manual**, p. Peculiarities of a Network with Several Dr.Web Servers.

   Dr.Web Server can be installed on any computer, not only on a computer functioning as a LAN server. General system requirements to this computer are described in p. System Requirements.

   On all protected stations including LAN servers, the same Dr.Web Agent version is installed. Difference is in the installing anti-virus components list which is defined be the settings on the Server.

   To install Dr.Web Server and Dr.Web Agent, one-time access (physical or via tools of remote control and program launch) to the correspondent computers is required. All further steps will be taken from the anti-virus network administrator’s workplace (which can also be outside the local network) and will not require access to Dr.Web Servers and workstations.

   When planning the anti-virus network, it is also recommended that a list of persons is made up, who are to be granted access to the Control Center as required by their job duties, as well as a list of roles with respective responsibilities assigned to each role. An administrative group shall be created for every role. Specific administrators can be linked with the roles by having their accounts placed into administrative groups. If necessary, administrative groups (roles) can be grouped hierarchically as a multilevel system allowing for individual editing of administrative permissions for each level.

   For detailed guidelines of how to manage administrative groups and permissions see **Administrator Manual**, Chapter 5: Anti-Virus Network Administrators

2. According to the constructed plan, define what products for what operating systems should be installed on corresponding network nodes. Detailed information on the supported products is given in the Distribution Kit section.

   All required products can be obtained as a box solution or downloaded at the official web site of Doctor Web at https://download.drweb.com.

   Dr.Web Agents for stations under Android OS, Linux OS, macOS can be also installed from the standalone packages and in the sequel get connected to the centralized Dr.Web Server. Description of the Agent settings is given in the corresponding **User manuals**.

3. Install Dr.Web Server general distribution kit on selected computer or computers. Installation description is given in p. Installing Dr.Web Server.

   Dr.Web Security Control Center is installed with the Server.

   By default, Dr.Web Server automatically starts after installation and every time after restarting the operating system.

4. If anti-virus network will include protected stations under Android OS, Linux OS, macOS, install Dr.Web Server extra distribution kit on all computers with Dr.Web Server general distribution kit installed.
5. Install and configure the Proxy Server, if necessary. Description is given in p. Installing Proxy Server.
6. To configure the Server and anti-virus software on stations, connect to the Server via Dr.Web Security Control Center.

   > Dr.Web Security Control Center can be opened on any computer, not just on the one with Dr.Web Server installed. It is enough to have a network connection with a computer on which the Server is installed.

   Control Center is available at the following address:
   `http://`*<Server_Address>*`:9080`

   or

   `https://`*<Server_Address>*`:9081`

   where *<Server_Address>* is the IP address or domain name for the computer on which Dr.Web Server is installed.

   In the authorisation request dialogue window, specify the administrator's credentials. For default administrator:

   - Name—**admin**.
   - Password:
     - for Windows OS—password that was set during the Server installation.
     - for UNIX system-based OS—password that was automatically created during the Server installation (see also p. Installing Dr.Web Server for UNIX® System-Based OS).

   On successful connect to the Server, the main window of the Control Center will be opened (detailed description see in the **Administrator Manual**, in p. Dr.Web Security Control Center).

7. Perform the initial configuration of the Server (detailed description of the Server settings is given in the **Administrator Manual**, in p. Chapter 8: Configuring Dr.Web Server):

   a. In the License Manager section, add one or several license keys and propagate them on corresponding groups, particularly on the **Everyone** group. The step is obligatory if the license key was not set during the Server installation.

   b. In the General repository configuration section, set the components of anti-virus network to update from Dr.Web GUS. In the Repository state section, update products in the

Server repository. Update might take a long time to complete. Wait for the end of the update process before continuing the further configuring.

c. The **Administrating → Dr.Web Server** page contain the information on the Server version. If a new version is available, update the Server as described in the **Administrator manual**, in p. Updating Dr.Web Server and Restoring from the Backup.

d. If necessary, set up the Network connections to change default network settings used for interaction of all anti-virus network components.

e. If necessary, set up the list of the Servers administrators. The external administrators authentication is also available. For more details see the **Administrator Manual**, in Chapter 5: Anti-Virus Network Administrators.

f. Before using the anti-virus software, it is recommended to change the settings of the backup folder for the Server critical data (see **Administrator Manual**, p. Setting Dr.Web Server Schedule). It is recommended to keep the backup folder on another local disk to reduce the risk of losing the Server software files and backup copies at the same time.

8. Specify settings and configuration of anti-virus software for workstations (detailed description of groups and stations setup is given in the **Administrator Manual**, in Chapter 6 and Chapter 7):

   a. If necessary, create user groups of stations.

   b. Configure settings of the **Everyone** group and created user groups. Particularly, configure installing components section.

9. Install Dr.Web Agent software on workstations.

   In the Installation Files section, look through the list of supported files for the Agent installation. Select suitable for you installation option based on stations operating system, remote installation ability, option to specify the Server settings during the Agent installation, etc. For example:

   - If users install the anti-virus independently, use personal installation packages which are created vie the Control Center separately for each station. This type of packages also can be sent to users by email directly from the Control Center. Connection of stations to the Server perform automatically after the installation.
   - If you need to install the anti-virus on several stations within one user group, you can use the group installation package which is created via the Control Center in a single copy for multiple stations of a certain group.
   - For the remote installation via the network on a station or on several stations simultaneously (for stations under Windows OS only), use the network installer. The installation is performed via the Control Center.
   - Also you can perform the remote installation via the network on a station or on several stations simultaneously via the Active Directory service. For this, use Dr.Web Agent installer for networks with Active Directory, which is supported together with Dr.Web Enterprise Security Suite distribution kit but separately from the Server installer.
   - If you need to reduce the load on a communication channel between the Server and stations during the installation, you can use the full installer that perform the installation of the Agent and protection components at a time.

- Installation on stations under Android OS, Linux OS, macOS can be performed locally by the general rules. Also, already installed standalone product can be connected to the Server according to the corresponding configuration.

> To be able to use the full installer for Windows OS as well as installers for operating systems other than Windows OS, it is necessary that additional ("extra") distribution kit of Dr.Web Server is installed first.
>
> To guarantee that Dr.Web Agent works properly on a server Windows OS starting from Windows Server 2016, make sure to manually disable Windows Defender using group policies.

10. Agents establish a connection with the Server immediately after the installation. Anti-virus workstations are authorised at the Server according to the set policy (see **Administrator Manual**, p. New Stations Approval Policy):

    a. For installation from installation packages and also for automatic approval on the Server, workstations automatically get registration at first connect to the Server, and additional approval is not required.

    b. For installation from installer and manual access approval, new workstations should be approved by an administrator manually to be registered at the Server. At this, new workstations are not connected automatically, but placed by the Server into the newbies group.

11. After connecting to the Server and receiving settings, corresponding set of anti-virus components specified in the primary group settings are installed on the station.

> To finish the installation of workstation components, computer restart required.

12. Configuring stations and anti-virus software is also available after the installation (detailed description is given in the **Administrator Manual**, in Chapter 7).

3.2. Setting the Network Connections

General Information

The following clients are connected to Dr.Web Server:

- Dr.Web Agents
- Network Installers of Dr.Web Agents
- Neighbor Dr.Web Servers
- Dr.Web Proxy servers.

Connection is always initiated by a client.

The following schemas for connection to the Server are available:

1. Using Direct connections.

   This approach has a lot of advantages, but it is not preferable in some situations (also, there are some situations, that are not compatible with this approach).

2. Using Server Detection Service.

   Clients use this Service by default (if the other is not set obviously).

   You can use this approach, if the resetting of all system is needed, in particular, if you need to move the Server to another computer or change the IP-address of a computer with the Server.

3. Using the SRV protocol.

   This approach allows to search the Server by name of a computer or Server service via the SRV records at DNS server.

If you configure the anti-virus network for using the direct connections, the Server Detection Service can be disabled. To do this, at the transport settings (**Administration** → **Dr.Web Server configuration** → the **Network** tab → the **Transport** tab) leave the **Cluster address** field empty.

Firewall Setup

For anti-virus network components communication, all ports and interfaces, which are used by this components, must be opened on all computers in the anti-virus network.

During the Server installation, the installer automatically adds ports and interfaces of the Server to exceptions of Windows operating system firewall.

If any other firewall besides built-in Windows firewall is in use on a computer, the network administrator should set up it manually.

3.2.1. Direct Connections

Dr.Web Server Setup

In the Server settings the address must be set (see the **Appendices** document, p. Appendix E. The Specification of Network Addresses) to listen for accepting incoming TCP-connections.

You can specify this parameter in the following Servers settings: **Administration** → **Dr.Web Server configuration** → **Network** tab → **Transport** tab → **Address** field.

By default, the following parameters are set to "listen" by the Server:

- **Address**: empty value—use *all network interfaces* for this computer, on which the Server is installed.

- **Port**: `2193`—use the `2193` port.

> The 2193 port is registered for Dr.Web Enterprise Management Service in IANA.

For the proper functioning of all Dr.Web Enterprise Security Suite anti-virus network, it is enough for the Server to listen at least one TCP-port, which is known by all clients.

Dr.Web Agent Setup

During the Agent installation, the Server address (IP-address or hostname of the computer, on which the Server is launched) can be directly set in installation parameters:

`drwinst /server` <*Server_Address*>

For the Agent installation it is recommended to use the Server name, registered in DNS service. This will simplify the setting of the anti-virus network in case of moving Dr.Web Server to another computer.

By default the `drwinst` instruction launched without parameters will scan the network for Dr.Web Servers and will try to install Agent from the first found Server (the *Multicasting* mode with using Server Detection Service).

Thus, the Server address become known for the Agent during installation.

You can change the Server address in the Agent settings manually later.

3.2.2. Dr.Web Server Detection Service

In this connection scheme, client does not know the Server address preliminary. Before establishing each connection, the Server will be searched in the network. To do this, the client sends the broadcast query and waits for the respond, that includes Server address. After the client gets respond, it will establish a connection with the Server.

To realize this scheme, the Server must "listen" the network for such queries.

Several variants of realization of this scheme is available. Most important is that the Server search method at the clients side must be matched with the Server respond part.

The *Multicast over UDP* mode is used by default in Dr.Web Enterprise Security Suite:

1. Server gets registered in the multicast group with an address specified in the Server settings.
2. Agents during Server search, send multicast requests to the group address specified at the step 1.

Server listens by default (similarly to direct connections): `udp/231.0.0.1:2193`

This parameter is set at the Servers settings: **Administration** → **Dr.Web Server configuration** → the **Network** tab → the **Transport** tab → **Multicast group** field.

3.2.3. Using SRV Protocol

Clients under Windows OS support SRV client network protocol (format description is given in the **Appendices** document, p. Appendix E. The Specification of Network Addresses).

Accessing the Server via the SRV records are implemented by the following way:

1. During the Server installation, registration in Active Directory domain is set up, installer registers corresponding SRV record on DNS server.

   > SRV record is registered on DNS server according to the RFC2782 (see http://tools.ietf.org/html/rfc2782).

2. In a request for connecting the Server, client specifies access via the `srv` protocol.

   For example, launch the Agent installer:

   - with explicit specification of a service name `myservice`:
     ```
     drwinst /server "srv/myservice"
     ```
   - without specification of a service name. At this, SRV record with the `drwcs` default name will be searched.
     ```
     drwinst /server "srv/"
     ```

3. Transparently for the user, the client uses functional of SRV protocol to access to the Server.

   > If the Server is not specified directly, the `drwcs` is used by default as a name of the service.

3.3. Providing a Secure Connection

3.3.1. Traffic Encryption and Compression

The encryption mode is used to ensure the security for data transmitted over an insecure channel and to avoid the possible disclosure of valuable information and substitution of software downloaded to the protected stations.

Dr.Web Enterprise Security Suite anti-virus network uses the following cryptographic means:

- Electronic digital signature (GOST R 34.10-2001).
- Asymmetric encryption (VKO GOST R 34.10-2001 – RFC 4357).
- Symmetric encryption (GOST 28147-89).
- Cryptographic hash function (GOST R 34.11-94).

Dr.Web Enterprise Security Suite anti-virus network allows to encrypt the traffic between Server and the following clients:

- Dr.Web Agents.
- Dr.Web Agent installers.
- Neighbor Dr.Web Servers.
- Dr.Web Proxy-servers.

As traffic between components, in particular the traffic between Servers, can be considerable, the anti-virus network provides for compression of this traffic. The setting of the compression policy and the compatibility of settings on different clients are the same as those for encryption.

Settings Compatibility Policy

The encryption and compression policy is set separately for each component of the anti-virus network, at this, settings of other components should be compatible with the settings of the Server.

When coordinating encryption and compression settings on the Server and a client, please consider that certain combinations are incompatible and, if selected, will result in disconnecting the client from the Server.

Table 3-1 describes what settings provide the connection between the Server and the clients encrypted/compressed (+), when the connection will be non-encrypted/uncompressed (–) and what combinations are incompatible (**Error**).

Table 3-1. Compatibility of the encryption and compression policy settings

Client settings	**Server settings**		
	Yes	**Possible**	**No**
Yes	+	+	Error
Possible	+	+	–
No	Error	–	–

Encryption of traffic creates a considerable load on computers those capacities are close to the minimal system requirements for the components installed on them. So, when traffic encryption is not required to provide additional security, you can disable this mode.

To disable encryption mode, you should step by step switch the Server and other components to the **Possible** mode first, avoiding formation of incompatible client-Server pairs.

Using the compression mode reduces traffic, but considerably increases the memory usage and the computational load on computers, more than the encryption.

Connection via Dr.Web Proxy Server

If you want to connect clients to the Server via Dr.Web Proxy server, you must consider the encryption and compression settings on all three components. At this:

- Settings of the Server and the Proxy server (here it plays a role of a client) must be conformed by the table 3-1.
- Settings of the client and the Proxy server (here it plays a role of the Server) must be conformed by the table 3-1.

Ability to establish a connection via the Proxy server depends on a version of the Server and a client that support certain encryption technologies:

- If the Server and the client support TLS encryption that is used in the version 11.0.2, it is enough to perform the above conditions to establish the working connection.
- If one of the components does not support TLS encryption: the Server and/or a client has the version 10 or earlier providing the GHOST encryption, the addition check is performed according to the table 3-2.

Table 3-2. Compatibility of the encryption and compression policy settings at using the Proxy server

Client connection settings	Server connection settings			
	Nothing	**Compression**	**Encryption**	**All**
Nothing	Normal mode	Normal mode	Error	Error
Compression	Normal mode	Normal mode	Error	Error
Encryption	Error	Error	Transparent mode	Error
All	Error	Error	Error	Transparent mode

Abbreviations

Server and client connection settings	
Nothing	Neither compression nor encryption is supported.
Compression	Only compression is supported.
Encryption	Only encryption is supported.

All	Both, compression and encryption are supported.
Result connection	
Normal mode	Established connection implies the operation in the normal mode—using commands processing and caching.
Transparent mode	Established connection implies the operation in the transparent mode—without commands processing and without caching. Encryption protocol version is taken minimal: if one of the components (the Server or the Agent) has version 11, and the other has version 10, the encryption of version 10 is used.
Error	Connection of the Proxy server both with the Server and with the client will be terminated.

Thus, if the Server and the Agent have different version: one has version 11, and other has version 10 and previous, then the following limitations are applied to the established connections via the Proxy server:

- Data can be cached on the Proxy server only if both of connections with the Server and with the client are established without using the encryption.
- The encryption will be used only if both of connections with the Server and with the client are established with using the encryption and the same compression parameters (compression is used for both connections or not used for both of them).

Encryption and Compression Settings on the Server

To specify the encryption and compression policies of the Server

1. Select the **Administration** item in the main menu of the Control Center.
2. In the opened window, click **Dr.Web Server configuration** in the control menu.
3. On the **Network** → **Transport** tab, select the necessary variant in the **Encryption** and **Compression** drop-down lists:
   - **Yes**—enables obligatory traffic encryption (or compression) with all clients (is set by default for encryption, if the parameter has not been modified during the Server installation).
   - **Possible**—instructs to encrypt (or compress) traffic with those components those settings do not prohibit it.
   - **No**—encryption (or compression) is not supported (is set by default for compression, if the parameter has not been modified during the Server installation).

> ⚠ When configuring encryption and compression on the Server, please consider the features of the clients which are planning to be connected to this Server. Not all clients support traffic encryption and compression.

Encryption and Compression Settings on the Proxy Server

To centralized specify the encryption and compression policies for the Proxy server

> If the Proxy server is not connected to Dr.Web Server for remote settings control, configure the connection as described in p. Connecting the Proxy Server to Dr.Web Server.

1. Open the Control Center of the managing Server for the Proxy server.
2. Select the **Anti-virus network** item in the main menu of the Control Center, in the hierarchical list of the opened window, click the name of the Proxy server settings of which you want to edit or its primary group if the Proxy server settings are inherited.
3. In the opened control menu, select **Dr.Web Proxy server**. Settings section opens.
4. Go to the **Listen** tab.
5. In the **Settings for connection with clients** section, in the **Encryption** and **Compression** drop-down lists, select the encryption and compression modes of traffic for channels between Proxy server and served clients: Agents and Agent installers.
6. In the **Settings for connection with Dr.Web Servers** section, you can specify the list of Servers to which the traffic will be forwarded. Select the necessary Server in the list and click ✎ on the toolbar to edit the settings for connection with selected Dr.Web Server. In the opened window, in the **Encryption** and **Compression** drop-down lists, select the encryption and compression modes of traffic for channels between Proxy server and the specified Server.
7. To save all the specified settings, click **Save**.

To locally specify the encryption and compression policies for the Proxy server

> If the Proxy server is connected to the managing Dr.Web Server for remote configuration, then the Proxy server configuration file will be rewritten according to the settings received from the Server. In this case, you must configure the settings remotely from the Server or disable the option that allows to receive configuration from this Server.
>
> Description of the `drwcsd-proxy.conf` configuration file is given in the **Appendices** document, in the Appendix G4.

1. On the computer with the Proxy server installed, open the `drwcsd-proxy.conf` configuration file.
2. Edit the settings for encryption and compressions for connections with clients and the Servers.
3. Restart the Proxy server:
   - For Windows OS:
     - If the Proxy server is run as a service of Windows OS, restart the service by the standard means of the system.

  - ▫ If the Proxy server is run in console, press CTRL+BREAK.

- For UNIX system-based OS:
  - ▫ Send the `SIGHUP` signal to the Proxy server daemon.
  - ▫ Execute the following command:

  For Linux OS:

  ```
  /etc/init.d/dwcp_proxy restart
  ```

  For FreeBSD OS:

  ```
  /usr/local/etc/rc.d/dwcp_proxy restart
  ```

Encryption and Compression Settings on Stations

To centralized specify the encryption and compression policies of stations

1. Select the **Anti-virus Network** item in the main menu of the Control Center, then click the name of a group or a station in the hierarchical list of the opened window.
2. In the opened control menu, select **Connection parameters**.
3. On the **General** tab, in the **Compression mode** and **Encryption mode** drop-down lists, select one of the following:
   - **Yes**—enables obligatory traffic encryption (or compression) with the Server.
   - **Possible**—instructs to encrypt (or compress) traffic with the Server if the Server settings do not prohibit it.
   - **No**—encryption (or compression) is not supported.
4. Click **Save**.
5. The changes will take effect as soon as the settings will be passed to stations. If stations are offline at the time of changing the settings, the changes will be passed as soon as stations connect to the Server.

Dr.Web Agent for Windows

Encryption and compression settings can be set at the Agent installation:

- At the remote installation from the Control Center, encryption and compression mode is set directly in the **Network installation** section settings.
- At local installation, the GUI installer does not provide encryption and compression changing, but these settings can be set using the command line switches during the installer launch (see the **Applications**, p. H2. Network Installer).

After the Agent installation, you cannot change encryption and compression settings locally on station. By default, the **Possible** mode is set (if other value has not been set at the installation), i.e. encryption and compression usage depends on the Server settings. However, the Agent settings can be changed via the Control Center (see above).

Dr.Web Anti-virus for Android

Dr.Web Anti-virus for Android does not support neither encryption nor compression. Connection will be impossible if the **Yes** value is specified for encryption and/or compression at the Server or the Proxy server (for connection via the Proxy server).

Dr.Web Anti-virus for Linux

At the anti-virus installation, you cannot change encryption and compression settings. By default, the **Possible** mode is set.

After the anti-virus installation, you can change encryption and compression settings locally on station only in the command line mode. You can find the description of a command line mode and corresponding switches in the **Dr.Web for Linux User Manual**.

Also, the station settings can be changed via the Control Center (see above).

Dr.Web Anti-virus for macOS

You cannot change encryption and compression settings locally on station. By default, the **Possible** mode is set, i.e. encryption and compression usage depends on the Server settings

The station settings can be changed via the Control Center (see above).

3.3.2. Tools to Ensure Secure Connection

At Dr.Web Server installation, the following tools are created to ensure the secure connection between components of the anti-virus network:

1. **The Server private encryption key** `drwcsd.pri`**.**

   Is stored at the Server and is not passed to other components of the anti-virus network.

   If the private key is lost, the connection between components of the anti-virus network must be restored manually (create all the keys and certificates and also propagate them to all components of the network).

   The private key is used in the following ways:

   a) *Creating pubic keys and certificates.*

      The public encryption key and the certificate are created automatically from the private encryption key during the Server installation. At this, the private key can be either newly created or used existing (for example, from the previous Server installation). Also encryption keys and certificates can be created at any time using the `drwsign` Server utility (see the **Appendices** document, p. H9.1. Digital Keys and Certificates Generation Utility).

Information on public keys and certificates is given below.

b) *The Server authentication*.

The Server is authenticated by remote clients on the basis of an electronic digital signature (once within each connection).

The Server performs the digital sign of a message by a private key and sends the message to a client. A client checks the signature of a received message using the certificate.

c) *Decrypting the data*.

When the traffic between the Server and clients are encrypted, the decryption of the data sent by a client is performed at the Server using the private key.

2. **The Server public encryption key** `drwcsd.pub`**.**

Is available to all components of the anti-virus network. A public key is always can be generated from a private key (see above). At each creation from the same private key you will get the same public key.

Starting from the version 11 of the Server, a public key is used for connection with previous versions of clients. The rest of the functionality is transferred to a certificate, which, among other things, contains a public encryption key.

3. **The Server certificate** `drwcsd-certificate.pem`**.**

Is available to all components of the anti-virus network. Certificate contains a public encryption key. Certificate can be generated from a private key (see above). At each creation from the same private key you will get a new certificate.

Clients connected to the Server, are bind to a specific certificate, so if the certificate is lost on client, it can be restored only if the same certificate is used by any other network component: in this case, certificate can be copied to a client from the Server or from the other client.

Certificate is used in the following ways:

a) *The Server authentication*.

The Server is authenticated by remote clients on the basis of an electronic digital signature (once within each connection).

The Server performs the digital sign of a message by a private key and sends the message to a client. A client checks the signature of a received message using the certificate (particularly, a public key specified in the certificate). In the previous version of the Server, to do this, a public key was used directly.

A client must have one or several trusted certificates from the Server to which a client can be connected.

b) *Encrypting the data*.

When the traffic between the Server and clients are encrypted, the encryption of the data is performed by a client using a public key.

c) *Implementation of a TLS session between the Server and remote clients.*

d) *The Proxy server authentication.*

Dr.Web Proxy server is authenticated by remote clients on the basis of an electronic digital signature (once within each connection).

The Proxy server performs the digital sign of its certificates by a private key and a certificate of the Dr.Web Server. The client which trusts Dr.Web Server certificate will be automatically trust to certificates that are signed by it.

4. **Web server private key.**

Is stored at the Server and is not passed to other components of the anti-virus network. Usage details are given below.

5. **Web server certificate.**

Is available to all components of the anti-virus network.

Is used to implement a TLS session between web server and a browser (over HTTPS).

At the Server installation, on the basis of a private key of a web server, self-signed certificate is generated that will not be accepted by web browsers because it was not released by a well-known certification authority.

To make a secure connection (HTTPS) available, you must perform on of the following:

- Add a self-signed certificate to trusted certificates or to exclusions for all stations and web browsers on which the Control Center is opened.
- Get a certificate signed by a well-known certification authority.

3.3.3. Connecting Clients to Dr.Web Server

To be able to connect to Dr.Web Server, a client must have the Server certificate not depending on the encryption of traffic between the Server and a client.

The following clients can be connected to Dr.Web Server:

- **Dr.Web Agent.**

  For the centralized mode of the Agents with connection to the Dr.Web Server, the station must have one or several trusted certificates from the Server to which the Agent can be connected.

  Certificate that was used at installation and certificates received in the centralized settings from the Server are stored in the registry but the files of certificates are not used.

  The single file of a certificate can be added using the command line switch into the Agent installation folder (but not to the registry) and into the common list of used certificates. This certificate is used, among other things, to be able to connect to the Server in case an error in the centralized settings.

If the certificate is absent or the certificate in invalid, the Agent will not be able to connect to the Server but will remain operating and updating in the Mobile mode if it is allowed for this station.

- **Dr.Web Agent Installers.**

  When installing the Agent, together with the selected installation file, the Server certificate must be on a station.

  If you launch the installation package generated in the Control Center, the certificate is included into the installation package and additional specifying of the certificate file is not required.

  After the Agent installation, the certificate data are written into the registry and the certificate file itself is no longer used.

  If the certificate is absent or the certificate in invalid, the installer will not be able to install the Agent (applies to all types of the Agent installation files).

- **Neighbor Dr.Web Servers.**

  When establishing a connection between neighbor Dr.Web Servers of version 11, on each configuring Server you must specify the certificate of the Server connection to which is establishing (see the **Administrator Manual**, p. Setting Connections between Several Dr.Web Servers).

  If at least one certificate is absent or invalid, you will not be able to establish the multiserver connection.

- **Dr.Web Proxy servers.**

  To connect the Proxy server to Dr.Web Server with possibility of remote control via the Control Center, you must have a certificate on a station with the Proxy Server installed. At this, the Proxy server can also support encrypting.

  If the certificate is absent, the Proxy server will remain its operation but remote control and also encryption and caching will not available.

> In case of general update of the entire anti-virus network from a previous version that uses public keys to a new version that uses certificates, no other additional actions are required.
>
> Installation of the Agent distributed with the Server of version 11 with connecting to the Server of version 10 and vice versa is not recommended.

Chapter 4: Installation of Dr.Web Enterprise Security Suite Components

4.1. Installing Dr.Web Server

The installation of Dr.Web Server is the first step in the installation of Dr.Web Enterprise Security Suite anti-virus. Unless and until it is successfully installed, no other Dr.Web Enterprise Security Suite components can be installed.

Installation of full package of Dr.Web Server contains the following two steps:

1. Installation of *general distribution kit*. General distribution kit performs the installation of Dr.Web Server itself and includes anti-virus protection packages for stations under Windows OS only.
2. Installation of *extra distribution kit*. Extra distribution kit includes distributions of all enterprise products, which are provided for installation on protected stations under all supported OS. The package is installed as an additional on a computer with Dr.Web Server general distribution kit installed.

The installation procedure of Dr.Web Server depends on Server version (for Windows OS or for UNIX system-based OS).

All parameters set during the installation can be changed later by an anti-virus network administrator.

If the Server software is already installed on your computer, see the Upgrading Dr.Web Enterprise Security Suite for Windows® OS or Upgrading Dr.Web Enterprise Security Suite for UNIX® System-Based Systems sections correspondingly.

If the previously installed Server was removed before installing the Server software, contents of the repository will be deleted during installation and the new version will be installed. If the repository of the previous version by some reason was not removed, it is necessary to manually delete the contents of the repository before installing the new version of the Server and then renew the repository after installation.

The Server installation folder name must be set on the same language as specified in the language settings of Windows OS for the non-Unicode programs. Otherwise, the Server installation will not be completed.

The English language is an exception for the installation folder name.

Together with Dr.Web Server, Dr.Web Security Control Center is installed, which serves to manage the anti-virus network and set up the Server.

By default, Dr.Web Server will run automatically after the installation under Windows OS and must be started manually under UNIX system-based OS.

4.1.1. Installing Dr.Web Server for Windows® OS

Below is described the installation of Dr.Web Server for Windows OS. The set and the order of steps may somewhat differ depending on the distribution file version.

Before installing, please consider the following:

The distribution file and other files requested during the program installation should reside on local drives of the computer on which the Server software is installed; these files should be made accessible for the LocalSystem user.

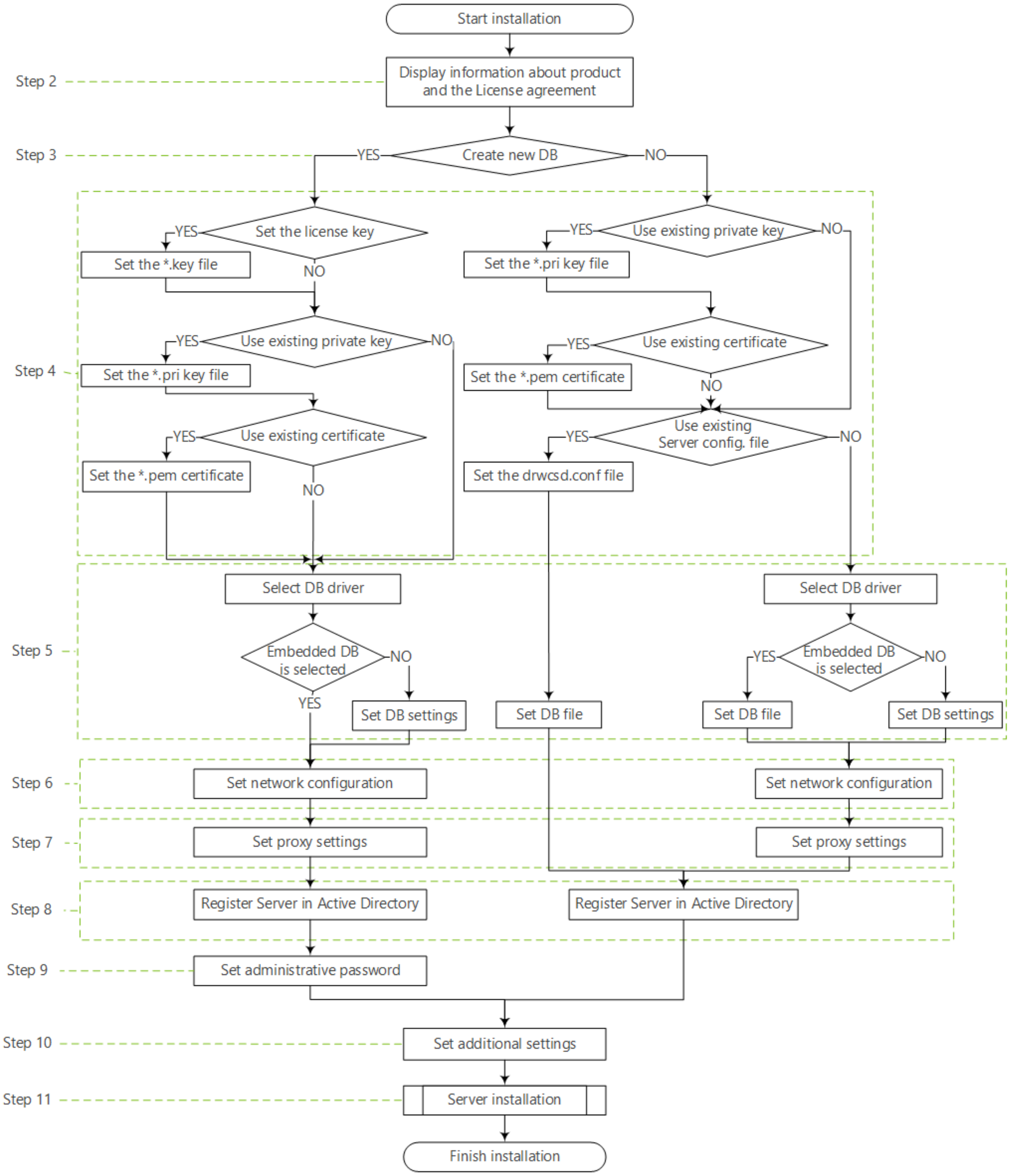
Dr.Web Server should be installed by a user with the administrator's rights to the computer.

After Dr.Web Server is installed it is necessary to update all Dr.Web Enterprise Security Suite components (see **Administrator manual**, p. Manual Update of Dr.Web Server Repository).

In case an external database is to be used it is necessary to create the database first and set the ODBC driver (see Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver).

Server installation module supports the product change mode. To add or remove separate components, e.g. database configuration drivers it is necessary to run the Server installer and select **Change**.

Figure 4-1 illustrates the flowchart of Dr.Web Server installation procedure. Steps in the flowchart correspond with the detailed description of the installation procedure shown below.



Picture 4-1. Dr.Web Server installation procedure flowchart (click any block in the flowchart to see its description)

To install Dr.Web Server on a computer operated by Windows OS:

1. Run the distribution file.

By default, installer uses the language of the operating system. If necessary, you can change the installation language on any step by selecting the corresponding option in the right upper part of the installer window.

2. A window with information on the product to install and the link to the license agreement text will be opened. When you read the agreement, to continue the installation, select **I accept the terms of the license agreement** and click **Next**.
3. In the next window, select which database will be used for the anti-virus network:
   - **Create a new database**—to create a new anti-virus network.
   - **Use the existing database**—to keep the database from the previous Server installation. You will be able to specify the database file later (see step **5**).
4. In the next window, setup the database.

   a) If at step **3** you have selected the **Create a new database** option, in the **New Database Parameters** window, specify the following settings:

   - The **Set the license key** flag allows to set Dr.Web Agent license key file during the Server installation.
     - If the flag is cleared, the Server installation is performed without the Agent license key. In this case, the license keys must be added after the Server installation via the License Manager.
     - If the flag is set, you must specify the path to the Agent license key file in the corresponding field.
   - The **Use existing private encryption key** flag allows to use the existing encryption keys, e.g., from the previous Server installation.
     - At the first Server installation, clear the **Use existing private encryption key** flag. New encryption keys and certificate will be automatically generated during the installation process.
     - If you are installing the Server for an existing anti-virus network, set the **Use existing private encryption key** flag and specify the path to the private key file in the corresponding field. At this, the public key file (content of the public key will match the content of the previous public key) and the certificate (at each creation from the same private key you will get a new certificate) will be automatically generated.
     - If you are installing the Server for an existing anti-virus network and using an existing private encryption key, set the **Use existing certificate** flag to specify the certificate file that was used previously. This allows for already installed Agents to connect to the new Server, because clients connected to the Server, are bind to a specific certificate (at each creation from the same private key you will get a new certificate). Otherwise, after the installation, it will be necessary to copy the new certificate to all workstations, on which Dr.Web Agents have been previously installed.
     - If an error occurs during the public key extraction, specify the path to the file with the corresponding public key manually in the **Public encryption key** opened field.

For evaluation purposes, you can use a demo key files. Click **Request the demo key** to go to the official web site of Doctor Web company and receive the demo license key files (see Demo key files).

b) If at step **3** you have selected the **Use the existing database** option, in the **Existing Database Parameters** window, specify the following settings:

- The **Use existing configuration file** flag allows to specify the Server settings.
  - If the flag is cleared, the Server configuration file with the default settings will be created.
  - If the flag is set, you must specify the path to the configuration file with the Server settings in the corresponding field.
- The **Use existing private encryption key** flag allows to use the existing encryption keys, e.g., from the previous Server installation.
  - At the first Server installation, clear the **Use existing private encryption key** flag. New encryption keys and certificate will be automatically generated during the installation process.
  - If you are installing the Server for an existing anti-virus network, set the **Use existing private encryption key** flag and specify the path to the private key file in the corresponding field. At this, the public key file (content of the public key will match the content of the previous public key) and the certificate (at each creation from the same private key you will get a new certificate) will be automatically generated.
  - If you are installing the Server for an existing anti-virus network and using an existing private encryption key, set the **Use existing certificate** flag to specify the certificate file that was used previously. This allows for already installed Agents to connect to the new Server, because clients connected to the Server, are bind to a specific certificate (at each creation from the same private key you will get a new certificate). Otherwise, after the installation, it will be necessary to copy the new certificate to all workstations, on which Dr.Web Agents have been previously installed.
  - If an error occurs during the public key extraction, specify the path to the file with the corresponding public key manually in the **Public encryption key** opened field.

For evaluation purposes, you can use a demo key files. Click **Request the demo key** to go to the official web site of Doctor Web company and receive the demo license key files (see Demo key files).

5. The **Database Driver** window allows you to adjust the parameters of the used database which depend on the database type specified at step **3** and the availability of the Server configuration file specified at step **4**.
   - If at step **3** you have selected the **Create a new database** option or for the **Use the existing database** option at step **4** you have not specified the path to the Server configuration file, select the driver to use. At this:
     - The **SQLite (embedded database)** option prescribes to use embedded facilities of Dr.Web Server. Additional parameters are not required.
     - The rest options imply usage of an external DB. You must specify corresponding parameters to configure the access to a DB. Parameters of DBMS are described in the

appendices (see Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver).

- If at step **3** you have selected the **Use the existing database** option and at step **4** you have specified the path to the Server configuration file, specify the path to the database file to use according to the specified Server configuration file.

6. If at step **3** you have selected the **Create a new database** option or for the **Use the existing database** option at step **4** you have not specified the path to the Server configuration file, the **Network Configuration** window will be opened. You can set up a network protocol for the Server (it is allowed to specify only one network protocol; additional protocols can be configured later).

   To specify the network settings from the predefined set, select one of the following variants from the drop-down list:

   - **Standard configuration** prescribes to use default settings on base of the Server detection service.
   - **Limited configuration** prescribes to limit the Server operation only to the internal network interface—`127.0.0.1`. With such settings the Server can be administrated only from the Control Center opened on the same computer, and communicate only with the Agent launched on the same computer. In future, after the Server settings have been checked out you will be able to change network settings.
   - **User-defined configuration** indicates what the following predefined setting are changed:
     - In the **Interface** and **Port** fields, specify the corresponding values to access the Server. Default interface is `0.0.0.0`, which means that the Server can be accessed via any interface.

   > By default the `2193` port is used.
   >
   > ---
   >
   > Addresses should be specified in the network addresses format described in the **Appendices** document, p. Appendix E. The Specification of Network Addresses.

     - Set the **Restrict access to Dr.Web Server** flag to limit the local access to the Server. The Agent Installers, Agents and other Servers (for existing anti-virus network built with Dr.Web Enterprise Security Suite) will not be able to access the Server. You can change these settings later via Dr.Web Security Control Center menu **Administration → Dr.Web Server configuration → Modules** tab.
     - Set the **Enable Dr.Web Server detection service** if you want the Server to answer broadcast and multicast requests from other Servers by IP address and service name specified in the corresponding fields below.

7. If at step **3** you have selected the **Create a new database** option or for the **Use the existing database** option at step **4** you have not specified the path to the Server configuration file, the **Proxy server** window will be opened to setup parameters of a proxy server usage when connecting to the Server:

   To connect to the Server via the proxy server, set the **Use proxy server** flag.

> The **Use proxy server** flag will be available only if the Server installation folder does not contain configuration files from the previous installation.

Specify the following parameters to setup a connection to the proxy server:

- **Proxy server address**—the proxy server address (obligatory field),
- **User name**, **Password**—user name and the password to access the proxy server, if the proxy server supports authorized connection.
- In the **Authorization method** drop-down list, select necessary method of authorization at proxy server, if the proxy server supports authorized connection.

8. If computer on which you are installing the Server is included into the Active Directory domain, in the next window you will be prompted to register Dr.Web Server in the Active Directory domain. During registration in Active Directory domain, the SRV record corresponding to Dr.Web Server, is created on DNS server. Further, clients can access Dr.Web Server via this SRV record.

   Specify the following parameters for the registration:

   - Set the **Register Dr.Web Server in the Active Directory** flag.
   - In the **Domain** field, specify the name of the Active Directory domain to register the Server in. If the domain is not specified, the domain in which the computer with installing Server is registered, is used.
   - In the **User name** and **Password** fields, specify Active Directory domain administrator credentials.

9. If at step **3** you have selected the **Create a new database** option, the **Administrative password** window will be opened. Specify the password for anti-virus network administrator which is created by default with the **admin** login and the full set of permissions to manage anti-virus network.

10. The next window notifies you that the Wizard is ready to install Dr.Web Server. If necessary, you can configure additional installation parameters. For this, click **Additional parameters** in the bottom if the window and specify the following settings:

    - On the **General** tab:
      - In the **Dr.Web Security Control Center interface language** drop-down list, select default interface language for Dr.Web Security Control Center.
      - In the **Dr.Web Agent interface language** drop-down list, select default interface language for Dr.Web Agent and anti-virus package components installing on stations.
      - Set the **Share Dr.Web Agent installation folder** flag to change the usage mode and the name of Agent shared installation folder (hidden name of shared resource is set by default).
      - Set the **Launch Dr.Web Server after installation is complete** flag to start the Server automatically after the installation.
      - Set the **Update repository after installation is complete** flag to update the Server repository automatically after the installation is complete.

- Set the **Send statistics to Doctor Web company** flag to send statistics on virus events to Doctor Web company.

- On the **Path** tab:
  - In the **Dr.Web Server installation folder** field, the folder to install the Server is specified. To change default folder, click **Browse** and select the necessary folder.
  - In the **Dr.Web Server backup folder** field, the folder to backup Server critical data according to the tasks from the Server schedule is specified. To change default folder, click **Browse** and select the necessary folder.
- On the **Components** tab, you can select the components you want to install.

> ⚠ If you are going to use the ODBC for Oracle as an external database, select the **Custom** option and disable the installation of Oracle client (in the **Database support** → **Oracle database driver** section) in the opened window.
>
> Otherwise, Oracle DB functioning will fail because of the libraries conflict.
>
> Platforms supported by the Oracle Client are listed on the web site of the vendor.

- On the **Log** tab, you can specify the settings for logging of the Server installation and operation.

After the additional parameters setup is finished, click **OK** to apply these changes or **Cancel** if no changes were made or to cancel specified changes.

11. Click **Install** to start the installation. Further actions of the installation program do not require user intervention.
12. Once the installation is complete, click **Finish**.

As a rule, Dr.Web Server can be managed via Dr.Web Security Control Center which acts as an interface for the Server.

In the **Programs** main menu of Windows OS installation wizard places the **Dr.Web Server** folder containing the following elements for configuration and managing the Server:

- The **Server control** folder contains the commands to start, restart and shut down the Server, as well as the commands to set up the logging parameters and other Server commands described in detail in Appendix H4. Dr.Web Server.
- **Web interface** item opens Dr.Web Security Control Center and connects to the Server installed at this computer (at the http://localhost:9080).
- **Documentation** item opens administrator documentation in HTML format.

Structure of the Server installation folder is described in the **Administrator Manual**, in the Dr.Web Server section.

4.1.2. Installing Dr.Web Server for UNIX® System-Based OS

Installation should be carried out in console under superuser account (**root**).

Package-based installation of Dr.Web Server on a UNIX system-based OS

1. To start installing the Server, use the following command:

   `./`*<distribution_file>*`.tar.gz.run`

   To launch the installation package, you can use command line switches. Parameters of command line launch are given in the **Appendices** document, p. H8. Dr.Web Server Installer for UNIX® System-Based OS

   By default, administrator's name is **admin**.

2. Next, the text of the license agreement presented. To proceed the installation, you must accept the license agreement.
3. On a request of backup folder, specify the path to the necessary folder or confirm default backup folder—`/var/tmp/drwcs`.
4. If the extra distribution kit is detected in the system, you will be informed about deletion of the extra distribution kit before installation of the Server package. You cannot continue the installation without deletion of extra distribution kit.
5. Then the program components will be installed on your computer. In the course of the installation you can be asked to confirm some actions as the administrator.
6. During the installation, a random password is generated for the main administrator. After the installation is complete, this password is printed in the console into the Server installation results.

   Created administrator password is saved in the Server database. If necessary, you can refine this password via the database management tools if you use external database or via the `drwidbsh` utility for the embedded database (for more details, see the **Applications** document, p. Restoring the Password of Dr.Web Enterprise Security Suite Administrator).

   In the course of the installation of Dr.Web Server for **FreeBSD** OS an `rc` script `/usr/local/etc/rc.d/drwcsd` will be created.

   Use the following commands:

   - `/usr/local/etc/rc.d/drwcsd stop`—manually stop the Server,
   - `/usr/local/etc/rc.d/drwcsd start`—manually start the Server.

⚠ Please note, during the Server installation, the license key is not specified. License keys must be added after installation of the Server, via the License Manager.

Configuring Astra Linux of Version 1.6 for Installing Dr.Web Server in the ESE Mode

At the installation of the Server in the Astra Linux OS of version 1.6 that operates in the ESE (Enclosed Software Environment) mode, you may be failed to launch the installer because the public encryption key of Dr.Web Server is not in the trusted keys list. In this case, you must pre-configure the ESE mode, and restart the installer.

To pre-configure the ESE mode

1. Install the `astra-digsig-oldkeys` package from the OS installation disk, if the package is not yet installed.
2. Place the public encryption key of Dr.Web Server to the `/etc/digsig/keys/legacy/keys` directory (if the directory is missing, you must create it).
3. Run the following command:

```
# update-initramfs -k all -u
```

4. Restart the system.

4.1.3. Installing Dr.Web Server Extra Distribution Kit

Installation of extra distribution kit must be performed on a computer with Dr.Web Server general distribution kit installed. Description of Server general distribution kit installation is given in the Installing Dr.Web Server for Windows® OS and Installing Dr.Web Server for UNIX® System-Based OS sections.

⚠ Extra distribution kit must be installed from the same type of package as a general distribution kit.

To install Dr.Web Server extra distribution kit on a computer operated by Windows OS

1. Run the distribution file.
2. The **Dr.Web Server Extra** window with information about the program and the license agreement to be installed will be opened. When you read the agreement, to continue the installation, select **I accept the terms of the license agreement** and click **Install**.
3. Installation of extra distribution kit begins. If no errors occur, further actions of the installation program do not require user intervention.

4. Once the installation is complete, click **Finish**. Computer reboot is not required.

To install Dr.Web Server extra distribution kit on a computer operated by UNIX system-based OS

1. Run the distribution file via the following command:

   `./<distribution_file>.tar.gz.run`
2. Next, the text of the license agreement presented. To proceed the installation, you must accept the license agreement.
3. Then the program components will be installed on your computer.

4.2. Installing Dr.Web Agent

⚠ Dr.Web Agent should be installed under Administrator account of the respective computer.

If Dr.Web Agent is installed on the computer, you must uninstall the Agent before the installation.

To guarantee that Dr.Web Agent works properly on a server Windows OS starting from Windows Server 2016, make sure to manually disable Windows Defender using group policies.

Dr.Web Agent can be installed on a workstation by one of the following ways:

1. Locally.

   Local installation is performed directly on a user's computer or mobile device. Installation may be implemented either by administrator or by user.
2. Remotely.

   Remote installation is available for stations under Windows OS only and performed in the Control Center through the LAN. Installation is implemented by an anti-virus network administrator. At this, user intervention is not required.

Dr.Web Agent installation over Dr.Web standalone product on stations under Windows OS

If a standalone Dr.Web product of 7/8/9/10/11 version is installed on the station, the installation of Agent for Dr.Web Enterprise Security Suite version 11.0.2 is preformed according to the following scheme:

- If the Agent installer or installation package is launched in the GUI mode on the station with standalone product of 7.0/8.0/9.0/9.1/10.0 version installed, the installer of corresponding version of installed product will be launched. After this, the user is prompted to enter the confirmation code and uninstall the product. After the OS reboot, the GUI version of Agent installer for Dr.Web Enterprise Security Suite version 11.0.2 is launched.

- If the Agent installer is launched in the background mode on a station with standalone product of 7.0/8.0/9.0/9.1/10.0 version installed, this will not incur any actions. In case of remote installation, the installer returns the message to the Control Center about standalone product of previous version installed. In this case, you must remove standalone product manually and install the Agent for Dr.Web Enterprise Security Suite version 11.0.2 by any of available ways.
- If the Agent installer is launched on a station with standalone product of 11.0 version, the installed product switches from the standalone mode to the centralized protection mode. After connection and authorization on the Server, the updates, new settings and the list of installing components can be received, depending on which, reboot may required.

For installation of Dr.Web Agent on LAN servers and cluster computers, consider the following:

- For installation on computers which implement terminal server functions (the **Terminal Services** are installed on Windows OS), to provide Agents operation in user's terminal sessions, Agents software is recommended to be installed locally, via the Add or Remove Programs Wizard on **Control Panel** of Windows OS. Remote installation in this case can cause Remote Desktop Protocol errors.
- It is not recommended to install SpIDer Gate, Office Control, SpIDer Mail and Dr.Web Firewall components on servers which implement significant network functions (domain controllers, license distribution servers and etc.) to avoid probable conflicts between network services and internal components of Dr.Web anti-virus.
- Installation of the Agent on a cluster must be performed separately on each cluster node.
- The operation principles for Agents and anti-virus package on the cluster node are similar to those on a standard LAN server, thus, it is not recommended to install SpIDer Gate, SpIDer Mail and Dr.Web Firewall components on cluster nodes.
- If access to quorum resource of a cluster is severely restricted, it is recommended to exclude it from the scan by the SpIDer Guard and confine by regular checks of the resource via Scanner launched by scheduler or manually.

4.2.1. Installation Files

Installation Packages

Personal Installation Package

After a new stations account is created in the Control Center, a personal installation package for Dr.Web Agent installation is generated. Personal installation package contains Dr.Web Agent installer and the set of parameters for connecting to the Server and for authorization of the station at the Server.

Personal installation packages are available for protected stations under all operating systems which are supported by Dr.Web Enterprise Security Suite. At this, installation packages are generated in the Control Center in base of the Agent installer. Parameters for connecting to the Server and for authorization of the station at the Server are included into installation packages directly.

> ⚠ To have installation packages for operating systems other that Windows OS, you must install extra distribution kit of Dr.Web Server first.

Download link for Dr.Web Agent personal installation package for the concrete station is available:

1. After creating of a new station (see the **11** step in the Creation of a New Station Account section).
2. In any time after station creation:
   - in station properties,
   - in the **Selected objects** section for the station selected in hierarchical list.

Group Installation Package

Group installation package of the Agent is generated in the Control Center for installation on stations of a certain user group. At this, you can install the Agent on all stations under the same OS from the one group installation package.

Group installation package contains Dr.Web Agent installer, the set of parameters for connecting to the Server and also the identifier and the password of the user group into which the station will be included after the Agent installation. But parameters for the authorization of the station at the Server and anti-virus components are not included into the group installation package composition.

Download link for group installation package is available in the user group properties.

Installers

Agent installer differs from the installation package that it does not contain parameters for connecting to the Server and for authorization of the station at the Server.

The following types of Dr.Web Agent installers are provided:

- For stations under Windows OS, two type of installers are available:
  - `drwinst.exe` *Network Installer* performs the installation of the Agent only. After connecting ti the Server, the Agent downloads and installs necessary anti-virus package components. It is possible either local or remote installation of the Agent via the network installer.

The `drwinst.exe` Agent network installer resides in the `webmin/install` folder (the shared hidden resource by default) of Dr.Web Server installation folder. Network sharing at the 10 step during Dr.Web Server installation is set. You can change this resource further.

  - `drweb-11.05.2-`*<build>*`-esuite-agent-full-windows.exe` *Full Installer* performs the installation of the Agent and anti-virus package at a time.

- For stations under Android OS, Linux OS, macOS, installers for Dr.Web Agent installation similar to the stand-alone version are available.

Dr.Web Agent installers are available on the installation page of Dr.Web Security Control Center.

⚠ To have installers for operating systems other that Windows OS, and also for the full installer under Windows OS, you must install extra distribution kit of Dr.Web Server first.

Installation Page

At the installation page of Dr.Web Security Control Center you can download:

1. Dr.Web Agent installer.

   Installers for protected stations under all operating systems which are supported by Dr.Web Enterprise Security Suite are located in corresponding named folders.

2. The `drwcsd.pub` public encryption key.
3. The `drwcsd-certificate.pem` Server certificate.

From any computer with network access to the Server, installation page is available at the following address:

`http://`*<Server_address>*`:`*<port_number>*`/install/`

where *<Server_address>* is the IP address or DNS name of the computer on which Dr.Web Server is installed. And the *<port_number>* should be `9080` (or `9081` for https).

4.2.2. Local Installation of Dr.Web Agent

Local installation of Dr.Web Agent is performed directly on the user’s computer or mobile device. May be performed either by administrator of by user.

⚠ You must update the Server repository before the first installation of the Agent (see **Administrator manual**, p. Manual Updating of Dr.Web Enterprise Security Suite Components, p. **Checking for Updates**).

Stations under Android OS, Linux OS, macOS

For local installation of Dr.Web Agent on stations under Android OS, Linux OS, macOS the following means are available:

- Personal installation package created in the Control Center.
- Group installation package created in the Control Center.
- Installer of Dr.Web Agent.

When you choose the type of installing package, please note the following features:

a) When the personal installation package is created, Dr.Web Agent installer is provided for installation, and parameters for connecting to the Server and for authorization of the station at the Server are provided in the configuration file.

b) For installation via the installer, Dr.Web Agent is installed, but parameters for connecting to the Server and for authorization of the station at the Server are not provided.

Stations under Windows OS

For local installation of Dr.Web Agent on stations under Windows OS, the following means are available:

- Personal installation package created in the Control Center `drweb_ess_`*<OS>*`_`*<station>*`.exe`.
- Group installation package created in the Control Center `drweb_ess_`*<OS>*`_`*<group>*`.exe`.
- Full installer of Dr.Web Agent `drweb-11.05.2-`*<build>*`-esuite-agent-full-windows.exe`.
- Network installer of Dr.Web Agent `drwinst.exe`.

When you choose the type of installing package, please note the following features:

a) For installation via the personal installation package, parameters for connecting to the Server and for authorization of the station at the Server are included into the personal installation package. Installation via the personal installation package is performed on base of the network installer from which the Agent only is installed. After connecting to the Server, the Agent downloads and installs the anti-virus package components.

b) For installation via the group installation package, parameters for connecting to the Server and also the identifier and the password of the user group into which the station will be included after the Agent installation, are included into the installation package. But parameters for the authorization of the station at the Server and anti-virus components are not included into the group installation package composition. After the Agent is installed, the Agent connects to the Server, during that, it is determined whether free stations are available in the user group, the group installation package of which has been used. If free stations are available, parameters for the authorization of the station at the Server are granted automatically.

c) For installation via the full installer, the Agent and anti-virus package are installed at a time. At this, parameters for connecting to the Server and for authorization of the station at the Server are not provided.

d) For installation via the network installer, the Agent only is installed. After connecting to the Server, the Agent downloads and installs the anti-virus package components. At this, parameters for connecting to the Server and for authorization of the station at the Server are not provided.

Comparative characteristics of installation files

Installation file		**Agent installation**	**Anti-virus package installation**	**Server connection parameters**	**Server authorization parameters**
Installation package	Personal	+	–	+	+
	Group	+	–	+	–
Installer	Network	+	–	–	–
	Full	+	+	–	–

To have installation packages and installers for operating systems other that Windows OS, and also for the full installer under Windows OS, you must install extra distribution kit of Dr.Web Server first.

You can also launch all types of the Agent installation files from the command line using the switches given in the **Appendices** document, p. H2. Network Installer.

4.2.2.1. Installing Dr.Web Agent via the Personal Installation Package

To install Dr.Web Agent on protected stations via the personal installation package:

1. Via the Control Center, create an account for a new station on the Server.
2. Send to a user the link on Dr.Web Agent personal installation package for corresponding operating system of a computer or mobile device, if a user performs Dr.Web Agent software installation directly.

For easy delivering of installation and configuration files, you can use the **Mailing of installation files** function (detailed information is given in the **Administrator Manual**, p. Mailing of Installation Files) to email messages with corresponding files.

3. Install Dr.Web Agent on a workstation.

Local installation of Dr.Web Agent on workstations is described in the **User Manual** for corresponding OS.

Dr.Web Agent should be installed by a user with the administrator rights to the computer.

If anti-virus software has already been installed on a workstation, then before starting installation the installer will attempt to remove it. If the attempt fails, the user will have to uninstall the anti-virus software from his computer by himself.

4. For stations under masOS, configure parameters of connection to Dr.Web Server locally.

   After installation of Dr.Web Agent on stations under other supported systems via the personal installation package, additional configuring is not required. Parameters of connection to the Server and authorization parameters are included into a personal installation package directly. After the Agent installation is complete, the station automatically connects to the Server.

Creation of a New Station Account

To create a user account or several user accounts, use Dr.Web Security Control Center.

When creating a user account, please note the name of the Server specified in the following sections of the Control Center:

1. **Administrating** → **Web server configuration** → the **Dr.Web Server address** field. This parameter value is used when generating the link on the Agent installation package.
   If the parameter value is not specified, when the DNS name (if available) or IP address of a computer on which the Control Center is opened, is used as a Server name to generate the link on Agent installer download.
2. **Administrating** → **Dr.Web Server configuration** → the **Network** tab → the **Download** tab → the **Dr.Web Server address** field. This parameter value is specified in the Agent installation packages and defines to which Server the Agent connects during installation.
   If the parameter value is not specified, when creating an installation package of the Agent, the name of the Server to which the Control Center connected is used. In this case, the Control Center must be connected to the Server using the IP-address of the domain for which you create an account (the Server address must not be specified as a loopback—`127.0.0.1`).

To create a new user via Dr.Web Security Control Center, do the following

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the toolbar, click **Add a network object** → **Create station** option. A pane for the new station account creation will be opened in the right part of the Control Center window.
3. In the **Number** entry field, specify the number of accounts to be created.
4. In the **Identifier** field, unique identifier of created station will be generated automatically. You can edit it, if necessary.
5. In the **Name** field, specify the station name that will be displayed in the anti-virus network hierarchical list. Further, after the station is connected with the Server, this name can be automatically changed to the station name which is specified locally.
6. In the **Password** and **Confirm Password** fields you can specify a password for accessing the Server by a station. If the password is not specified, it will be generated automatically.

   When creating more than one account, **Identifier**, **Name** and **Password** (**Confirm Password**) fields are set automatically and cannot be changed at the stage of station creation.

7. In the **Description** field, specify additional information about the customer. This parameter is optional.
8. In the **Groups** section, specify groups in which the created station will be included.
   - In the **Membership** list, you can configure the list of user groups into which the station will be included.
     By default, station is included into the **Everyone** group. If custom groups are available, you can include creating station into those groups with no limitations on the number of groups into which the station is included. To do this, set the flags next to the user group names in the **Membership** list.

   You cannot exclude stations from the **Everyone** group and from a primary group.

   To set a primary group for the creating station, click the icon of the corresponding group from the **Membership** list. The **1** will appear on the group icon.

   - In the **Policies** list, you can set the policy from which the creating station settings will be used.
     By default, the policy is not set. To specify the policy, set the flag next to the necessary policy. Station settings will be inherited from the settings of the current version of this policy. No more than one policy can be assigned to a station.
9. In the **Proxy server** section, you can configure the settings of Dr.Web Proxy server connected with this station.
   If you want to install the Proxy server on the creating station, set the **Create linked Proxy Server** flag and and specify the parameters of the Proxy server. The parameters are the same as when creating a Proxy server.

> When creating the station account, the Proxy account will be created in the Control Center. After the settings transmitted to the station, the Proxy server will be installed on this station in the background mode. The Agent will be connecting to the Server through the installed Proxy server only. The Proxy server usage will be transparent to a user.

10. Specify parameters of the **Security** section, if necessary. Parameters of this section are described in the **Administrator Manual**, in the p. Security.
11. Specify parameters of the **Location** section, if necessary.
12. Click **Save** in the upper right corner. The opened pane contains information about successful creation of a station, its ID and the following links:
    - The **Installation file** item contains the link for downloading Agent installer for this station.

> After a new station has been created, before the operating system of a station is set, in the section of distribution kit downloading, the links are presented separately for all OS that are supported by Dr.Web Enterprise Security Suite.
>
> ---
>
> Link for the Agent installation package downloading is also available:
>
> - in station properties after its creation,
> - in the **Selected objects** section for the station selected in hierarchical list.
>
> See also the Installation Files section.
>
> ---
>
> To have installation packages for operating systems other that Windows OS, you must install extra distribution kit of Dr.Web Server first.

- The **Configuration file** item contains the link for downloading the file with settings of connection to Dr.Web Server for stations under Android, macOS and Linux operating systems.
- The **Password** item contains the password to access this station to the Server. To view the password, click 👁.
- The **Proxy server password** item contains the password to access the Proxy server to the Server, if the station is created with the connected Proxy server (see step 9).
- In this window, the **Install** button is also available which is intended for remote installation of Dr.Web Agent Software via Dr.Web Security Control Center.

13. Installation of Dr.Web Anti-virus on workstations is described in the **User Manual** for corresponding OS.

Configuring Parameters of Connection to Dr.Web Server for Stations under macOS

1. In Dr.Web Anti-virus application menu, click **Preferences** and select **Mode**.
2. Set the **Enable central protection mode** flag.

3. Parameters of connection to the Server, such as IP address and authorization parameters at the Server, are specified automatically from the `install.cfg` configuration file that resides in the personal installation package.

   To use this file:

   a) Click **Other activation types** in the License Manager.

   b) Drag the configuration file to the opened window or click the dotted area to select the file.

   If the file is mounted, fields for entering the connection settings will be specified automatically.

4.2.2.2. Installing Dr.Web Agent via the Group Installation Package

To install Dr.Web Agent on protected stations via the group installation package

1. Via the Control Center, create a new user group on Dr.Web Server (detailed description of groups creation is given in the **Administrator Manual**, p. Creating and Deleting Groups). Also, you can use the existing group you have created before.
2. If necessary, in the License Manager assign the personal license key for the group. Otherwise, the group inherits a license key from its parent group.
3. Via the Control Center, create accounts for new stations on Dr.Web Server. At this, include new station accounts into the user group from the step 1 and make this group primary for them. You can create as much stations into the user group as free licenses are available for this group.
4. In the group properties, the link for the group installation package become available. Installation packages are divided according to the tariffs: one installation package for each operating system per a tariff.
5. Send to users the link on Dr.Web Agent installation package for corresponding operating system of a computer or mobile device, if users perform Dr.Web Agent software installation directly. At this, send the same group installation package for corresponding operation system to all users.
6. Install Dr.Web Agent on a workstation.

Local installation of Dr.Web Agent on workstations is described in the **User Manual** for corresponding OS.

Dr.Web Agent should be installed by a user with the administrator rights to the computer.

If anti-virus software has already been installed on a workstation, then before starting installation the installer will attempt to remove it. If the attempt fails, the user will have to uninstall the anti-virus software from his computer by himself.

7. After the Agent is installed, the Agent connects to the Server specified in the group installation package. At first connection to the Server, it is determined whether free stations are available in the user group, the group installation package of which has been used for the Agent installation. The number of free stations is defined by the number of accounts in this group, which have not expired. At each connection of a group installation package, the number of free stations is recalculated to provide the actual information.

   a) If free stations are available, parameters for the authorization of the station at the Server are granted automatically. This procedure does not require any additional administrator intervention.

   b) If free stations are not available in this group, the installation is terminated with corresponding notification of a user.

4.2.2.3. Installing Dr.Web Agent via the Installer

Agent installer differs from the installation package that it does not contain parameters for connecting to the Server and for authorization of the station at the Server.

Dr.Web Agent installers are available on the installation page of Dr.Web Security Control Center.

> To have installers for operating systems other that Windows OS, and also for the full installer under Windows OS, you must install extra distribution kit of Dr.Web Server first.

Local Installation on Stations under Android OS, Linux OS, macOS

Under Android OS, Linux OS, macOS, installers for Dr.Web Agent installation similar to the stand-alone version are available.

> Local installation of Dr.Web Agent on workstations is described in the **User Manual** for corresponding OS.

If you perform the installation via the installer without the configuration file, you must specify the Server address to connect on station manually.

You can either specify authorization parameters manually or leave them blank. At this, the following variants of connection to the Server are available:

Setup option	Authorization parameters
Specified manually	Attempt of automatic authorization according to the specified parameters is performed.

Setup option	Authorization parameters
Not specified	Authorization mode on the Server depends on the Server settings for connecting new stations (for more details, see the **Administration Manual**, p. New Stations Approval Policy).

To specify authorization parameters manually, you must create a new station account in the Control Center first. At this, the installation package become available, which contains configuration file with connection and authorization parameters. It is recommended to use installation package instead of the installer.

Local Installation on Stations under Windows OS

The following types of Dr.Web Agent installers are provided:

- `drwinst.exe` *Network installer* performs the installation of the Agent only. After connecting ti the Server, the Agent downloads and installs necessary anti-virus package components.
- `drweb-11.05.2-`<*build*>`-esuite-agent-full-windows.exe` *Full Installer* performs the installation of the Agent and anti-virus package at a time.

If you use these installers, you can either specify parameters of authorization and connection to the Server manually or leave them blank.

To specify authorization parameters manually, you must create a new station account in the Control Center first. At this, the installation package become available. If there is no need to install via the full distribution kit or via network installer, it is recommended to use installation package instead of the installer.

The following variants of connection to the Server are available:

Setup option	Server address	Authorization parameters
Specified manually	The station addresses to the specified Server directly.	Attempt of automatic authorization according to the specified parameters is performed.
Not specified	Agent searches for the Server in the network based on the Server detection service. Attempt to connect to the first found Server is performed.	Authorization mode on the Server depends on the Server settings for connecting new stations (for more details, see the **Administration Manual**, p. New Stations Approval Policy).

The **User Manual** for Windows OS describes Dr.Web Agent installation via the full installer and via the installation package.

It is recommended to perform the installation via the network installer by the anti-virus network administrator.

Local Installation via the Network Installer under Windows OS

The `drwinst.exe` Agent network installer is provided to install the Agent under Windows OS only.

If the network installer is run in the normal installation mode (i.e. without the `/instMode remove` switch) on stations where the installation has already been performed, this will not incur any actions. The installer program terminates with a help window, contains available switches.

There are two modes of installation via the Network installer:

1. *Background mode*—runs if the background mode switch is specified.
2. *Graphical mode*—default mode. Runs if the background mode switch is not specified.

With the network installer, you can also install Dr.Web Agent on a workstation remotely via Dr.Web Security Control Center (see p. Remote Installation of Dr.Web Agent).

To install Dr.Web Agent on a workstation in the background mode of the installer

1. From the workstation, on which you want to install the anti-virus software, enter the network folder of the Agent installation (by default at the Server installation, it is the `webmin/install` folder of the Server installation folder, further it can be changed) or download from the installation page of the Control Center the `drwinst.exe` executable file and `drwcsd-certificate.pem` certificate. Run the `drwinst.exe` file with the `/silent yes` background mode switch.

   By default, if the `drwinst.exe` file launched without Server connection parameters, it will use the *Multicast* mode to scan the network for Dr.Web Servers and will try to install the Agent from the first found Server.

   When you use the *Multicast* mode to find active Servers, the Agent installation is performed from the first found Server. At this, if the public encryption key does not match the Server encryption key, installation will be failed. In this case, directly specify the Server address (as described below).

   If you need to install the Agent on the same computer on which the Server is installed, you must directly specify the Server address in the installer launch parameters, because the Server may not be found when searching via multicast request.

   The `drwinst.exe` file also may be used with the optional command line switches:

   - If the *Multicast* mode is not used, it is recommended to specify a domain name for Dr.Web Server directly (it must be registered on the DNS service):

```
drwinst /silent yes /server <Server_DNS_name>
```

It makes the configuration of the anti-virus network more easy especially in case you reinstall Dr.Web Server on a different computer.

- You can expressly specify the Server address as follows:

```
drwinst /silent yes /server 192.168.1.3
```

- Using the `/regagent yes` switch during the installation will allow you to register the Agent in the **Add or Remove Programs** list.

> ! The complete list of Network Installer parameters is describe in the **Appendices** document, p. H2. Network Installer.

2. After the installation is completed, the software of the Agent is installed on a computer (anti-virus package is not installed yet).
3. After the station has been approved at the Server (if it is required by the Server settings), the anti-virus package will be automatically installed.
4. Restart the computer on Agent request.

To install Dr.Web Agent on a workstation in the graphical mode of the installer

From the workstation, on which you want to install the anti-virus software, enter the network folder of the Agent installation (by default at the Server installation, it is the `webmin/install` folder of the Server installation folder, further it can be changed) or download from the installation page of the Control Center the `drwinst.exe` executable file and `drwcsd-certificate.pem` certificate. Run the `drwinst.exe` file.

A window of the Installation wizard of Dr.Web Agent will be opened. Further actions on the Agent installation on the stations via the graphical mode of the network installer are similar to the actions on the installation via the installation package, but without Server connection settings, if they have not been specified in the corresponding command line switch.

> ! Installation of the Agent on workstations is described in the **Dr.Web® Agent for Windows. User Manual**.

4.2.3. Remote Installation of Dr.Web Agent under Windows® OS

Dr.Web Enterprise Security Suite anti-virus allows to detect the computers which are not yet protected by Dr.Web Enterprise Security Suite, and in certain cases to install such protection remotely.

Remote installation is available in the following two variants:

- Via the Control Center.

- Via the Active Directory service, if the service is used in the LAN.

Remote installation of Dr.Web Agents is possible only on workstations operated by Windows OS (see the **Appendices** document, p. Appendix A. The Complete List of Supported OS Versions) except Starter and Home editions.

Remote installation of Dr.Web Agents is possible only from the Control Center opened under Windows OS (see the **Appendices** document, p. Appendix A. The Complete List of Supported OS Versions).

To install the anti-virus software on workstations, you must have administrator rights on the correspondent computers.

For remote installation via the Control Center, if the workstations are inside a domain and the domain administrative account is used for the installation, you must turn on file and printer sharing on workstations (how to find this option for different Windows OS versions, see in the table below).

If the remote stations are outside a domain, or if the local account is used during the installation, then for some of Windows OS, the extra configuration of the remote stations is required.

Extra Configuration for Remote Installation to a Station outside a Domain or Using the Local Account

Specified options can reduce remote station security. It is strongly recommended to examine functions of these options before editing the system settings or do not use remote installation and install the Agent manually.

After you configure remote workstation, it is recommended to return all changed settings into values before editing to not violate the basic policy of operating system security.

To install the Agent to a remote workstation outside a domain, or/and using the local account, do the following on the computer where you want to install the Agent:

Operating System	Configuration	
Windows XP	Setup the mode of access to shared files	Modern view: **Start** → **Settings** → **Control Panel** → **Appearance and Themes** → **Folder Properties** → the **View** tab → clear the **Use Simple Sharing (recommended)** flag.
		Classical view:

Operating System	Configuration	
		Start → **Settings** → **Control Panel** → **Folder Properties** → the **View** tab → clear the **Use Simple Sharing (recommended)** flag.
	Set the mode of network authentication model in the local policies	Modern view: **Start** → **Settings** → **Control Panel** → **Performance and Maintenance** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
		Classical view: **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Settings** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
	Disable the Windows Firewall on the station before remote installation.	
Windows Server 2003	Disable the Windows Firewall on the station before remote installation.	
Windows Vista Windows Server 2008	Enable the File sharing option	Modern view: **Start** → **Settings** → **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Sharing and discovery** → **File Sharing** → **Enable**.
		Classical view: **Start** → **Settings** → **Control Panel** → **Network and Sharing Center** → **Sharing and discovery** → **File Sharing** → **Enable**.
	Set the mode of network authentication model in the local policies	Modern view: **Start** → **Settings** → **Control Panel** → **System and Maintenance** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
		Classical view: **Start** → **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Settings** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
	Add the **LocalAccountTokenFilterPolicy** key: a) In the register editor, open the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch. If the **LocalAccountTokenFilterPolicy** record does not exist, in	

Operating System	Configuration	
	the **Edit** menu, select **Add** and specify the **DWORD** value. Enter the **LocalAccountTokenFilterPolicy** value and press ENTER. b) In the **LocalAccountTokenFilterPolicy** item context menu, select **Change**. c) In the **Value** field, set the **1** value and click **OK**. Reboot is not required.	
Windows 7 Windows Server 2008 R2	Turn on file and printer sharing	Modern view: **Start → Control Panel → Network and Internet → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**.
		Classical view: **Start → Control Panel → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**.
	Set the mode of network authentication model in the local policies	Modern view: **Start → Control Panel → System and Security → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
		Classical view: **Start → Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Settings → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
	Add the **LocalAccountTokenFilterPolicy** key: a) In the register editor, open the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch. If the **LocalAccountTokenFilterPolicy** record does not exist, in the **Edit** menu, select **Add** and specify the **DWORD** value. Enter the **LocalAccountTokenFilterPolicy** value and press ENTER. b) In the **LocalAccountTokenFilterPolicy** item context menu, select **Change**. c) In the **Value** field, set the **1** value and click **OK**. Reboot is not required.	
Windows 8 Windows 8.1 Windows Server 2012	Turn on file and printer sharing	Modern view: **Settings → Control Panel → Network and Internet → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**.

Operating System	Configuration	
Windows Server 2012 R2 Windows 10		Classical view: **Settings** → **Control Panel** → **Network and Sharing Center** → **Change advanced sharing settings** → **File and Printer Sharing** → **Turn on file and printer sharing**.
	Set the mode of network authentication model in the local policies	Modern view: **Settings** → **Control Panel** → **System and Security** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
		Classical view: **Settings** → **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
	Add the **LocalAccountTokenFilterPolicy** key: a) In the register editor, open the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch. If the **LocalAccountTokenFilterPolicy** record does not exist, in the **Edit** menu, select **Add** and specify the **DWORD** value. Enter the **LocalAccountTokenFilterPolicy** value and press ENTER. b) In the **LocalAccountTokenFilterPolicy** item context menu, select **Change**. c) In the **Value** field, set the **1** value and click **OK**. Reboot is not required.	

If user account at the remote computer has the empty password, set the access policy with empty password in local policies: **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Accounts: Limit local account use of blank passwords to console logon only** → **Disabled**.

4.2.3.1. Installing Dr.Web Agent Software via Dr.Web Security Control Center

The following means of remote Agent installation on network workstations are available:

1. Installation via the Network Scanner.

   Allows to perform preliminary search of unprotected computers in the network and installation Dr.Web Agents on them.

2. Installation using the Network Installation tool.

Fits for cases, when address of station or groups of stations on which the Agent will be installed, is previously known.

3. Installation on stations with specified ID.

   Allows to install Agents for selected accounts (including all new accounts) with specified ID and password for Server access on stations and groups of stations.

> ⚠ For proper operation of Network Scanner and the **Network Installation** tool under Microsoft Internet Explorer browser, IP address and/or DNS name of computer with installed Dr.Web Server must be added to the trusted sites of browser, on which you open Control Center for remote installation.

Using the Network Scanner

In Dr.Web Security Control Center, the anti-virus network hierarchical list displays only those computers which are already included into the anti-virus network. The program allows also to discover computers which are not protected with Dr.Web Enterprise Security Suite and to install anti-virus components remotely.

To quickly install the Agent software on workstations, it is recommended to use Network Scanner (see **Administrator Manual**, p. Network Scanner) which searches for computers by IP addresses.

To install Dr.Web Agent via the Network Scanner

1. Open the Network Scanner. On the **Administration** menu of Dr.Web Security Control Center, select **Network scanner**. A **Network scanner** window with no data loaded will be opened.
2. Set the parameters to search for stations in the network. Detailed description of the parameters is given in **Administrator Manual**, the Network Scanner section.
3. Click **Start Scanner**. The catalog (hierarchical list) of computers demonstrating where Dr.Web Enterprise Security Suite anti-virus software is installed will be loaded into this window.
4. Unfold the catalog elements corresponding to workgroups (domains). All elements of the catalog corresponding to workgroups and individual stations are marked with different icons the meaning of which is given below.

Table 4-1. Icons of the Network scanner

Icon	Description
	Workgroups
⚠	The work groups containing inter alia computers on which Dr.Web Enterprise Security Suite anti-virus software can be installed.
🛡	Other groups containing protected or unavailable by network computers.
	Workstations
🖥	Active station with installed anti-virus software.
🖥●	Active station with unknown state of anti-virus software (there is no anti-virus software on a station or it was not detected).

You can also unfold catalog items corresponding to computers with the 🖥 icon, and check which program components are installed there.

5. In the **Network scanner** window, select an unprotected computer (or several unprotected computers by pressing CTRL or SHIFT buttons).

6. On the toolbar, click 🛡 **Install Dr.Web Agent**.

7. The **Network Installation** window will be opened to configure the Agent remote installation task.

8. In the **Stations addresses** field, specify IP addresses or DNS names of computers on which Dr.Web Agent will be installed. If you set several stations, use “;” or “,” as a separator (number of spaces around a separator is irrelevant).

   For installation on stations found via the Network Scanner, the address of station or several stations on which installation will be performed, are already specified in the **Stations addresses** field.

9. By default the Agent software is installed to the `%ProgramFiles%\DrWeb` folder. If necessary, specify another location in the **Dr.Web Agent Installation folder** field.

   It is recommended to specify the full path for unique identification of installation folder location. It is allowed to use environment variables in the path.

10. By default the **Dr.Web Server** field displays IP address or DNS name of Dr.Web Server to which Dr.Web Security Control Center is connected. If necessary, specify the Server address from which the anti-virus software will be installed. If you set several Dr.Web Servers, use “;” or “,” as a separator (number of spaces around a separator is irrelevant). Leave this field blank to use Dr.Web Server detecting service (*Multicast* mode).

⚠ If you need to install the Agent on the same computer on which the Server is installed, you must directly specify the address in the **Dr.Web Server** field, because the Server may not be found when searching via multicast request.

11. In the **Language** drop-down list, select the language of interface for Dr.Web Anti-virus which will be installed on stations.

12. In the **Simultaneous installations** field, specify the maximum number of stations to perform parallel installation.

13. In the **Installation timeout (sec.)** field, specify maximum time to wait for the Agent installation to complete in seconds. Valid values: 1-600. 180 seconds is set by default. If network channel capacity between the Server and the Agent is low, it is recommended to enlarge the value of this option.

14. If necessary, set the **Register Dr.Web Agent in the system list of installed software** flag.

15. In the **Installing components** section, select the components of anti-virus package which will be installed on stations.

16. In the **Compression** and **Encryption** sections, specify the parameters of traffic compression and encryption used by the Network Installer during installation of the Agent and anti-virus package. These settings also will be used by the Agent for interaction with the Server after the installation.

17. In the **Authorization on remote stations** section, specify the parameters of authorization to access the remote computers on which the Agent will be installed.

    You can set several administrator accounts. To add one more account, click + and specify authorization parameters fields. Similarly, for each new record.

    During Agent installation, the first account in the list is used at first. If installation under this account failed, the next account in the list is used, and etc.

18. After all necessary parameters have been specified, click **Install**.

> For launching the installation of the anti-virus software, the build-in service is used.
>
> ---
>
> The installation uses the network installer of the current Server that is located in the `webmin\install\windows` folder of the Server installation folder and SSL certificate `drwcsd-certificate.pem` located in the `etc` folder of the Server installation folder.

19. Dr.Web Agent will be installed on the selected workstations. After the workstation has been approved at the Server (if it is required by Dr.Web Server settings, see also **Administrator Manual** New Stations Approval Policy), the anti-virus package will be automatically installed.

20. Restart the computer on Agent request.

Using the Network Installation Tool

In case an anti-virus network is basically created and it is necessary to install the Agent software on certain computers, it is recommended to use **installation via network**:

1. Select the **Administration** item in the main menu. Then, in the opened window select the **Network installation** item in the control menu.

2. Further steps are similar to **8-21** above.

Installation for Accounts with Specified ID

To perform remote Agent installation for accounts with selected ID

1. When creating a new station account:
   a) Add a new station account or several station accounts (see Creation of a New User Account).
   b) Right after adding account, in the right part of a main window, the **Install Dr.Web Agent** pain opens. Click **OK**.
   c) The Network Scanner window opens.
   d) Further steps are similar to **2-21** above.
   e) After installation is complete, check if icons of corresponding stations are changed in the hierarchical list.
2. When using existing station account:
   a) In the hierarchical list of anti-virus network, select a new station or group of stations, for which Agents are not installed, or the **New** group (for installation on all new accounts).
   b) Click **Install Dr.Web Agent** on the toolbar.
   c) The Network Scanner window opens.
   d) Further steps are similar to **2-21** above.
   e) After installation is complete, check if icons of corresponding stations are changed in the hierarchical list.

> Agent installation on stations with selected ID is also available of group administrators.

> See the **Appendices** document, the Remote Installation Trouble Shooting section, if an error has occurred.

4.2.3.2. Installing Dr.Web Agent Software via Active Directory

If the **Active Directory** service is used in the LAN, you can remotely install the anti-virus Agent on workstations using this service.

> The Agent installation via Active Directory service is also available when using Distributed File System (see the **Appendices** document, p. Using DFS During Installation the Agent via the Active Directory section).

Dr.Web Agent Installation

To install the Agent using the Active Directory

1. Download a copy of Dr.Web Agent installer for networks with **Active Directory** at https://download.drweb.com/.
2. Install Dr.Web Agent on the local network server supporting the **Active Directory** service. This can be made in the command line mode **(A)** or in the graphic mode of the installer **(B)**.

> If you upgrade the Server, you do not have to upgrade Dr.Web Agent installer for networks with Active Directory. After upgrading the Server software, the Agents and the anti-virus software will be upgraded at the stations automatically.

(A) To Set All Necessary Installation Parameters in the Command Line Mode

Issue the following command with all necessary parameters and the obligatory parameter `/qn` which disables the graphic mode:

```
msiexec /a <package_name>.msi /qn [<parameters>]
```

The `/a` parameter launches installation of the administrative package.

Package name

The name of the installation package for the Agent through Active Directory usually has the following format:

```
drweb-11.05.4-<build>-esuite-agent-activedirectory.msi
```

Parameters:

`/qn`—disable the graphic mode. With this switch the following parameters are to be specified:

- `ESSERVERADDRESS=`*<DNS_name>*—set the address of Dr.Web Server to which the Agent is to be connected. For the possible formats see the **Appendices** document, p. Appendix E.
- `ESSERVERPATH=`*<full_filename>*—specify the full path to the certificate of the Server and the file name (by default `drwcsd-certificate.pem` in the `webmin/install` subfolder of the Server installation folder).
- `TARGETDIR`—the network folder for the Agent image (modified installation package), which will be select via the Group Policy Object Editor for the selected installation. This folder must have read and write access. The path should be given in the network addresses format even if the folder is a locally accessible resource; the folder should be accessible from the target stations.

> ⚠ Before administrative installation, in the destination directory for the Agent image (see the `TARGETDIR` parameter), you should not place installation files manually. The Agent Installer for networks with Active Directory (<*package_name*>`.msi`) and other files required for installation of the Agents on workstations, will be placed into the destination folder automatically during administrative installation. If these files are present in the destination folder before the administration installation, e.g., from the previous installations, when the similar files will be rewritten.
>
> If you need to perform administrative installation from the different Servers, it is recommended to specify different destination folders for each Server.

> After deployment the administrative package, in the <*destination_directory*>`\Program Files\DrWeb` directory, only the `README.txt` file must resides.

Examples:

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=servername.net ESSERVERPATH=\
\win_serv\drwcs_inst\drwcsd-certificate.pem TARGETDIR=\\comp\share
```

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:
\Program Files\DrWeb Server\webmin\install\drwcsd-certificate.pem"
TARGETDIR=\\comp\share
```

These parameters can alternatively be set in the graphic mode of the installer.

Next on a local network server, where Active Directory administrative tools are installed, appoint installation of the package (see procedure below).

(B) To Set All Necessary Installation Parameters in the Graphic Mode

> ⚠ Before administrative installation, make sure that the destination directory for the Agent image does not contain Dr.Web Agent Installer for networks with **Active Directory** (<*package_name*>`.msi`).

> After deployment the administrative package, in the <*destination_directory*>`\Program Files\DrWeb` directory, only the `README.txt` file must reside.

1. Issue the command

   ```
   msiexec /a <path_to_installer>\<package_name>.msi
   ```

2. An **InstallShield Wizard** window with information on the program selected for installation will be opened. Click **Next**.

> The Agent Installer uses the language specified in the language settings of a computer.

3. In the next window, specify the DNS name (preferred form) or the IP address of Dr.Web Server (see the **Appendices** document, p. Appendix E). Specify the location of the public key file of the Server (`drwcsd.pub`). Click **Next**.
4. In the next window type the name of a network catalog, to which the image of the Agent is planned to be written. The path should be specified in the network addresses format even if the catalog is a locally accessible resource; the catalog should be accessible from the target stations. Click **Install**.
5. After installation is finished, the settings window displays which helps you configure installation of the package on network workstations.

Installation of the Package on Selected Workstations

1. In **Control Panel** (or in the **Start** menu for Windows 2003/2008/2012/2012R2 Server OS, in the **Start** → **Programs** menu for the Windows 2000 Server OS), select **Administrative Tools** → **Active Directory Users and Computers** (when you install Agent in the graphic mode, this window displays automatically).
2. In the domain containing the computers on which Dr.Web Agents are to be installed, create an organizational unit (hereinafter OU), name it, for example, ESS. To do this, in the domain context menu, select **New** → **Organizational unit**. In the opened window, type the new unit name and click **OK**. Include the computers, on which the Agent is to be installed, into this unit.
3. Open the group policy editor. To do this:

   a) for Windows 2000/2003 Server OS: on the OU context menu, select **Properties**. In the opened window go to the **Group Policy** tab.

   b) for Windows 2008 Server OS: select **Start** → **Administrative tools** → **Group Policy management**.
4. For the created OU, set the group policy. To do this:

   a) for Windows 2000/2003 Server OS: click **Add** and create an element named ESS policy. Double-click it.

   b) for Windows 2008/2012/2012R2 Server OS: on the OU context menu, select **Create a GPO in this domain, and Link it here**. In the opened window, specify the name of the new group policy object and click **OK**. In the new group policy context menu, select **Edit**.
5. In the **Group Policy Object Editor** window, specify the settings for the group policy created on step 4. To do this:

   a) for Windows 2000/2003 Server OS: in the hierarchical tree, select **Computer Configuration** → **Software Settings** → **Software Installations**.

   b) for Windows 2008/2012/2012R2 Server OS: in the hierarchical tree, select **Computer Configuration** → **Policies** → **Software Settings** → **Software Installations**.
6. On the context menu of **Software Installations**, select **New** → **Package**.

7. Specify the Agent installation package. To do this, specify the address of the network shared resource which contains the Agent image you created during the administrative installation. The path should be specified in the network addresses format even if the catalog is a locally accessible resource). Click **OK**.
8. A **Deploy Software** window will be opened. Select the **Assigned** option. Click **OK**.
9. In the **Group Policy Object Editor** window, select the added package. On the context menu of this element, select **Properties**.
10. In the opened package properties window, select the **Deployment** tab. Click the **Advanced** button.
11. An **Advanced Deployment Options** window will be opened.
    - Set the **Ignore language when deploying this package** flag.
    - If you plan to install Dr.Web Agent via the customize msi package on 64-bit OS, set the **Make this 32-bit x86 application available to Win64 machines** flag.
12. Click **OK** twice.
13. Dr.Web Agent will be installed on selected computers at their next registration in the domain.

Policies Assignment in Consideration of Previous Agent Installations

When you assign an Active Directory policy to install the Agent, you should consider a possibility, that the Agent is already installed at the station. There are three possible options:

1. **Dr.Web Agent is not installed at the station**.

   After policies assignment, the Agent will be installed by general rules.
2. **Dr.Web Agent is already installed at the station without using the Active Directory service**.

   After Active Directory policy assignment, installed Agent will remain at the station.

   > In this case, the Agent is installed at the station, but for the Active Directory service Agent is not installed. So, after every station startup, attempt of unsuccessful Agent installation will be repeated.

   To install the Agent via the Active Directory, you must uninstall the Agent manually (or via the Control Center) and assign the Active Directory policy for this station repeatedly.
3. **Dr.Web Agent is already installed at the station via the Active Directory**.

   Repeated assignment of a policy to a stations with Dr.Web Agent installed via the Active Directory service is not performed.

   Thus, policies assignment will not take any affect to the anti-virus software state at the station.

4.3. Installing NAP Validator

Dr.Web NAP Validator checks health of anti-virus software on protected workstations. It is installed on the computer where a configured NAP server resides.

To install NAP Validator

1. Run the installation file. In the dialog window, select the language to use during install. Select **English** and click **Next**.
2. On the Welcome page of the **InstallShield Wizard**, click **Next**.
3. On the **License Agreement** page, read the agreement. To accept the agreement and proceed with the installation, select **I accept the terms of the license agreement** and click **Next**. To exit the wizard, click **Cancel**.
4. On the next page, specify Dr.Web Server IP **Address** and **Port** and click **Next**.
5. Click **Install**. The installation begins.
6. When installation completes, click **Finish**.

After you install Dr.Web NAP Validator, add Dr.Web Server to the trusted NAP servers group.

To add Dr.Web Server to the trusted NAP servers group

1. To open NAP server configuration component, run the `nps.msc` command.
2. In the **Remediation Servers Group** section, click **Add**.
3. In the dialog window, enter the name for the new remedial server and Dr.Web Server IP address.
4. Click **OK** to save changes.

4.4. Installing Proxy Server

One or several Proxy servers can be included into the anti-virus network.

When choosing a computer to install the Proxy server, consider that the Proxy server should be accessible from all networks and segments which require data redirection between them.

You can install the Proxy server under Windows OS by one of the following ways:

- Automatically within Dr.Web Agent for Windows installation

  The installation is performed from a personal installation package of Dr.Web Agent, during creation of which the settings for the installation of connected Proxy server were specified. In this case, the Proxy server is installed automatically in the background mode.
- Automatically on a station with Dr.Web Agent for Windows installed

In the Control center, configure the connected Proxy installation for the selected station. The Proxy server will be installed on a station automatically in the background mode.

- Manually via the graphical installer

  The installation is performed manually by an administrator on any suitable network station. No other components of the anti-virus network may be installed at this station.

You can install the Proxy server under UNIX system-based OS only manually using the installer.

4.4.1. Connecting the Proxy Server to Dr.Web Server

Starting from version 11, Dr.Web Proxy Server can be connected to Dr.Web Server to configure settings remotely and to support the traffic encryption.

Connection Settings

Connection of the Proxy server to Dr.Web Server requires the following:

- **The Server certificate** `drwcsd-certificate.pem`.

  The Proxy server must have all certificates of all Servers to which the Proxy server connects and to which the client traffic is forwarded.

  - The Server certificate is required to connect to the Server for remote settings configuration and to support the traffic encryption between the Server and the Proxy server.
  - The Proxy server certificate is signed by the Server certificate and private key (the procedure is performed automatically on the Server after connection, and no administrator interception is required) and is required to connect Agents and to support the traffic encryption between the Agents and the Proxy server.

  All the Server certificates are stored on the Proxy server in the `drwcsd-proxy-trusted.list` configuration file in the following format (the certificates records are separated by one or more empty lines):

```
[<certificate_1>]


[<certificate_2>]


[<certificate_3>]

...
```

- **The Server address.**

  The Proxy server connects to all Dr.Web Servers that are specified in its configuration file for the client traffic forwarding. But accepting settings are allowed only from a specific set of connected Servers that are marked as managing. If several Servers are marked as managing, then Proxy server connects to all the Servers by rotation until it gets the first valid (not empty) configuration.

- **Identifier and password to access the Server.**

  Credentials are available after creation of the Proxy server account via the Control Center (see Creating of the Proxy Server Account).

  ⚠ Proxy server identifier and password are used in a single copy. You must create the Proxy server accounts with the same credentials on all Servers to which the Proxy server connects.

  Credentials are stored on the Proxy server in the `drwcsd-proxy.auth` configuration file in the following format:

  ```
  [<Proxy_server_ID>]

  [<Proxy_server_password>]
  ```

Connecting the Proxy Server to Dr.Web Server

⚠ To be able to connect Dr.Web Proxy server, you must enable corresponding protocol at Dr.Web Server. To do this, in the Control Center in the **Administration → Dr.Web Server configuration → Modules** section, set the **Dr.Web Proxy server protocol** flag, save the settings and restart the Server.

Automatically within installation under Windows OS

- If the Proxy server is installing within the Agent installation or on the station with the Agent installed, when connection to the Server is established automatically.
- If the Proxy server is installed via the graphical installer under Windows OS, when connection to the Server is established automatically using the credentials specified by administrator in the installer settings.

  After the Proxy server installation, the files for the connection to the Server are located by default in the following folder: `%ALLUSERSPROFILE%/Doctor Web/drwcs/etc`.

Manually for the installation under UNIX system-based OS

1. Install the Proxy server for UNIX system-based OS according to the procedure described in the Installing Proxy Server via the Installer section.

2. Create the Proxy server account using the Control Center as described in the Creating of the Proxy Server Account section.
3. Copy the Server certificate on the computer with the Proxy server installed.
4. In the `drwcsd-proxy-trusted.list` configuration file, specify the certificate copied on the computer at step 3: copy the contents of the certificate file and paste it into the configuration file according to the format above.
5. In the `drwcsd-proxy.auth` configuration file, specify the Server connection settings for the account created at step 2 according to the format above.

   The `drwcsd-proxy-trusted.list` and `drwcsd-proxy.auth` files must be located in the following directories:

   - for Linux OS: `/var/opt/drwcs/etc`
   - for FreeBSD OS: `/var/drwcs/etc`

   For the files, set the following permissions:

   ```
   drwcsd-proxy-trusted.list 0644 drwcs:drwcs

   drwcsd-proxy.auth 0600 drwcs:drwcs
   ```

4.4.2. Creating of the Proxy Server Account

> The administrator must create the Proxy server accounts on each Server to which the Proxy is going to connect (and forward the traffic).

To create the Proxy server account via Dr.Web Security Control Center

1. For the parent group into which you are going to create the Proxy server, specify the settings as described in the **Administrator Manual**, in the Remote Configuration of the Proxy Server section. In this case, the specified settings will be inherited by the Proxy server at connect. You can specify these settings after creation of the Proxy server account (as for the parent group in case of inheritance, and personally for the Proxy server itself), but before the connection of the Proxy server to the creating account.

   > If the settings have not been specified before the Proxy server connection, the configuration file will not be downloaded. Proxy server uses the current configuration until the configuration on the connected Server is set, provided that the Server is allowed to manage the configuration.

2. Select the **Anti-virus network** item in the main menu of the Control Center.
3. Steps to create the Proxy server depend on whether you want to install the Proxy server on an existing station with Dr.Web Agent or to install the Proxy server separately:

№	Actions	Install with the Agent	Install separately
a)	1. In the anti-virus network tree, select a station to install the connected Proxy-server. 2. On the properties pane of the selected station, go to the **Proxy server** section.	+	–
b)	1. In the anti-virus network tree, select a station to install the connected Proxy-server. 2. On the toolbar, select **Add a network object** → **Create Proxy server**.	+	+
c)	1. Make sure, no station is selected in the anti-virus network tree. 2. On the toolbar, select **Add a network object** → **Create Proxy server**.	+	+

If you are creating the Proxy server account for installation on a station with the Agent, the Proxy server installation will be performed automatically via the Agent in the background mode after the Proxy server account is created (see also Installing Proxy Server within Dr.Web Agent for Windows Installation).

If you are creating the Proxy server account for the separate installation (with no connection with the Agent), the Proxy server must be installed by administrator manually from the installation package supplied with the Server distribution kit.

4. In the **Identifier** field, unique identifier of created account will be generated automatically. You can edit it, if necessary.
5. In the **Name** field, specify the Proxy server name that will be displayed in the anti-virus network tree.
6. In the **Password** and **Confirm Password** fields, you can specify a password for accessing the Server by the Proxy server. If the password is not specified, it will be generated automatically.

Proxy server identifier and password are used in a single copy. You must create the Proxy server accounts with the same credentials on all Servers to which the Proxy server connects (see Connecting the Proxy Server to Dr.Web Server).

You cannot edit the identifier after creation of the Proxy server account.

7. For the steps 3.b) and 3.c), the **Station** field contains the existing station with the installed Agent to connect with this Proxy server.

   For the step 3.b), in the **Station** field, identifier of the selected station will be added automatically.

   For the step 3.c), the **Station** field is empty.

- To specify a station for the Proxy server installation, click ✎ and in the opened window, select the existing station from the anti-virus network tree.
- Leave the **Station** field blank to not link the Proxy server to any of the stations and connect the manually installed Proxy server. If the **Station** field already specified, click ✖ to remove the connected station.

8. In the **Membership** section, you can specify a group to include the created Proxy server. To change the group, set the flag next to the necessary group in the given list.

   The Proxy server can be included into one group only.

   You can select the pre-installed **Proxies** group and its subgroups only.

9. Click **Save**.

   The opened window contains information about successful creation of the Proxy server and its password to access the Server. To view the password, click 👁.

> Administrator needs identifier and password of the Proxy server account created in the Control Center to connect the Prosy server to the Server:
>
> - During the Proxy server installation via the graphical installer.
> - Manually after the Proxy server installation (for UNIX system-based OS only).

4.4.3. Installing Proxy Server within Dr.Web Agent for Windows Installation

To install the Proxy server together with the Dr.Web Agent for Windows

1. Specify the Proxy server settings as described in the **Administrator Manual**, p. Remote Configuration of the Proxy Server. Settings must be specified for the group in which you plan to create the Proxy server. In this case, the specified settings will be inherited by the Proxy server at creation. You also can specify these settings after the Proxy server creation (either for group for the inheritance or personally for the Proxy server), but before the connection of the Proxy server to the creating account.

> If the settings have not been specified before the Proxy server connection, the Proxy server uses the settings given by the installer. These settings prescribes to connect only to the Server from which the installation was performed.

2. Create a station account via the Control Center as described in the Installing Dr.Web Agent via the Personal Installation Package section. During the station creation, set the **Create linked Proxy server** flag and configure the given settings. Particularly, specify the group with the settings from step 1 to place the Proxy server.

> You can change the Proxy server identifier only at account creation.

3. On a station, launch the Agent installation from the personal installation package created at step 2.
4. After the installation, the Agent automatically downloads the Proxy server installer from the Server and launches it in the background mode on the same station. The Server certificate and address and also credentials to connect to the Server will be automatically written into the corresponding configuration files of the Proxy server. The Proxy server settings for the traffic forwarding will contain only the Server from which the installation was performed.
5. After the installation, the Proxy server connects to the Server from which the installation was performed, to get the complete configuration file. If the settings at the Server have not been specified at step 1, the configuration file will not be downloaded. Configuration specified by the installer will be used until the configuration on the connected Server is set.
6. The Agent connects to the Server only thought the installed Proxy server. The use of the proxy server will be transparent to the user.

4.4.4. Installing Proxy Server via the Installer

> ⚠ To install the Proxy server, you must have administrator permissions on this computer.

The Proxy Server Installation under Windows OS

1. Create the Proxy server account via the Control Center as described in the Creating of the Proxy Server Account section.
2. Copy the certificate of the Server to which the Proxy server will be connected (see Connecting the Proxy Server to Dr.Web Server) and the Proxy server installer supplied with the Server distribution kit, to a station where you plan to install.
3. Run the Proxy server installer. A window of **Installation Wizard** with information about the program to be installed will be opened. Click **Next**.
4. In the Proxy server parameters window, on the **General** tab, specify the following general parameters:
   - In the **Path to program data** field, if necessary, change the path to place the files used by the Proxy server: operation log, configuration files, cache. Path by default is `%PROGRAMDATA%/Doctor Web/drwcs`. To select another path, click **Browse**.
   - In the **Address to listen** field, specify the IP address that will be "listened" by the Proxy server. By default, it is any (`0.0.0.0`) value, which means "listen" for all interfaces.

   > Addresses should be specified in the network addresses format described in the **Appendices** document, p. Appendix E. The Specification of Network Addresses.

   - In the **Port** field, specify the number of port that will be "listened" by the Proxy server. By default, it is the `2193` port.

- Set the **Enable discovery** flag to enable the Server imitation mode. This mode allows clients to detect the Proxy server as Dr.Web Server during its search via multicast requests.
- Set the **Enable multicasting** flag so that the Proxy server replies to multicast requests addressed to the Server.
  - In the **Multicast group** field, specify an IP address of a multicast group to include the Proxy server. Specified interface will be listened by the Proxy server for interaction with clients during active Dr.Web Servers searching. If you leave this field blank, the Proxy server will not be included in any of multicast groups. Default multicast group to which the Server is included is `231.0.0.1`.
- In the **Settings for connection with clients** section:
  - In the **Encryption** drop-down list, select the encryption mode of traffic for channels between Proxy server and served clients: Agents and Agent installers.
  - In the **Compression** drop-down list, select the compression mode of traffic for channels between Proxy server and served clients: Agents and Agent installers. In the **Level** field, select the compression level (from 1 to 9).

5. On the **Cache** tab, specify the following caching parameters of the Proxy server:

   Set the **Enable caching** flag to cache the data transferred by the Proxy server and specify the following parameters:

   - In the **Revisions deleting interval (min)** field, specify the interval for deleting old revisions from the cache if their number exceeds the maximum number of revisions to remain. The value is set in minutes. Default is 60 minutes.
     - In the **Number of revisions to remain** field, specify the maximum number of each product revisions to remain in the cache after the cleanup. By default, 3 last revisions are stored, the older revisions are deleted.
   - In the **Unload interval of unused files (min)** field, specify the time interval in minutes for unloading unused files from the memory. Default is 10 minutes.
   - In the **Integrity check mode** drop-down list, select the integrity check mode for data stored in the cache:
     - **At startup**—at startup of the Proxy server (may take a long time).
     - **Idle**—at the downtime of the Proxy server operating.

   After you specified cache settings, click **Next**.

6. A window for configuring connections forwarding will be opened:

   In the **Redirection settings** section, specify an address of Dr.Web Server to which the connections that are established by the Proxy server, will be forwarded.

   Addresses should be specified in the network addresses format described in the **Appendices** document, p. Appendix E. The Specification of Network Addresses.

   - In the **Encryption** drop-down lists, select the encryption mode of traffic for channels between Proxy server and each of the specified Dr.Web Servers.

- In the **Compression** drop-down lists, select the compression mode of traffic for channels between Proxy server and each of the specified Dr.Web Servers. In the **Level** drop-down list, select the compression level (from 1 to 9).

To add one more Server into the traffic forwarding list, click + and specify the settings listed above.

To remove the Server from the traffic forwarding list, click − next to the Server you want to remove.

> After installation is complete, the Proxy server connects to the first Server from this section to receive the settings.
>
> If the Proxy server configuration is specified on the Server, all the settings specified in the installer will be replaced with the new configuration received from the Server.

After you specify forwarding settings, click **Next**.

7. A window with Dr.Web Server connection settings for remote control, opens.

   The connection is established with the first Server specified at step 6 for the traffic forwarding.

   - In the **Server certificate** field, specify the certificate file copied to the station on step 2. To select the file, click **Browse**.
   - In the **Identifier** and **Password** fields, specify credentials of the account created on the Server at step 1.

8. A window with information, that the Proxy server is ready to install, will be opened.

   If you want to change additional installation parameters, particularly, the Proxy server installation folder, click **Additional parameters**.

   To start the Proxy server installation, click **Install**.

9. Once the installation is complete, click **Exit**.

10. After the installation, the Proxy server connects to the first Server specified at step 6 to receive the complete configuration file. If the settings at the Server have not been specified, the configuration file will not be downloaded. Configuration specified by the installer will be used until the configuration on the connected Server is set.

The Proxy Server Installation under UNIX System-based OS

1. Run the Proxy server installer by executing the following command:

   ```
   ./<distribution_file>.tar.gz.run
   ```

2. To continue the installation, accept the licence agreement.
3. Specify the path to the Server certificate. You can also add the certificate after the Proxy server installation (see Connecting the Proxy Server to Dr.Web Server).
4. If necessary, you can use the configuration files from the previous Proxy server installation:

   - To use the default backup saved in `/var/tmp/drwcsd-proxy`, press ENTER.

- To use the backup from the other directory, specify the path to the backup manually.
- Also, you can install the Proxy server with the default settings not using the backup configuration from the previous version. For this, press 0.

5. After the Proxy server installation, if necessary, you can edit the corresponding configuration files manually (see Connecting the Proxy Server to Dr.Web Server).

Start and Stop

During the software installation under **FreeBSD** OS, an rc script `/usr/local/etc/rc.d/dwcp_proxy` is created. Use the commands:

- `/usr/local/etc/rc.d/dwcp_proxy stop`—to stop the Proxy server manually;
- `/usr/local/etc/rc.d/dwcp_proxy start`—to start the Proxy server manually.

During the installation for **Linux** OS, an `init` script `/etc/init.d/dwcp_proxy` to start and stop the Server will be created.

Chapter 5: Removal of Dr.Web Enterprise Security Suite Components

5.1. Removing Dr.Web Server

5.1.1. Removing Dr.Web Server for Windows® OS

To remove Dr.Web Server (general and extra distribution kits) or Dr.Web Security Control Center Extension software, run the installation file of the corresponding product of currently installed version. The installation program will automatically detect the software product and offer to remove it. To remove software, click **Remove**.

Dr.Web Server (general and extra distribution kits) and Dr.Web Security Control Center Extension software can also be removed using standard Windows OS tools via the **Control Panel** → **Add or Remove Programs**.

⚠ When removing the Server, configuration files, encryption keys and embedded database are back up only if you set the **Back up Dr.Web Server critical data** option.

5.1.2. Removing Dr.Web Server for UNIX® System-Based OS

⚠ Deinstallation should be carried out under the superuser account (**root**).

Removing general distribution kit of Dr.Web Server

To deinstall the Server of 10 and later versions, perform the following actions:

Server OS	Action
FreeBSD	Run the script: `/usr/local/etc/drweb.com/software/drweb-esuite.remove`
Linux	Run the script: `/etc/opt/drweb.com/software/drweb-esuite.remove`

At removing the Server under **FreeBSD** OS and **Linux** OS, the Server operations will be immediately terminated, the database, key and configuration files will be copied to `/var/tmp/drwcs` default backup folder (backup files list is given in the Upgrading Dr.Web Server for UNIX® System-Based OS section).

To cancel the back up, you need to define the `SKIP_BACKUP` environment variable. The variable may have any value. For example: `SKIP_BACKUP="x"`

Also, you can define this variable in the `common.conf` file.

Removing extra distribution kit of Dr.Web Server

To deinstall the extra distribution kit of the Server of 10 and later versions, perform the following actions:

Server OS	Action
FreeBSD	Run the script: `/usr/local/etc/drweb.com/software/drweb-esuite-extra.remove`
Linux	Run the script: `/etc/opt/drweb.com/software/drweb-esuite-extra.remove`

5.2. Removing Dr.Web Agent

Removing of Dr.Web Agent from protected stations can be performs by the following ways:

- For stations under Windows OS:
  - Remotely via the Control Center.
  - Locally on station.
  - Via the Active Directory service, if the Agent was installed using this service.
- For stations under Android OS, Linux OS, macOS—locally on stations.

Removing of Dr.Web Agent on workstations under Android OS, Linux OS, macOS is described in the **User Manual** for corresponding OS.

5.2.1. Removing Dr.Web Agent for Windows® OS

Uninstalling Dr.Web Agent and Anti-Virus Package Remotely

Remote installation and deinstallation of the Agent software is possible within a local network only and requires administrator’s rights in the local network.

If you uninstall the Agent and anti-virus package via the Control Center, the Quarantine will not be deleted from the station.

To uninstall the anti-virus software from a workstation (for Windows OS only)

1. Select the **Anti-virus network** item in the main menu of Dr.Web Security Control Center.
2. In the opened window select the necessary group or certain anti-virus stations.
3. Click **General** → **Uninstall Dr.Web Agent** in the toolbar of the anti-virus network catalog.
4. The Agent software and the anti-virus package will be removed from the workstations selected.

In case Agent removal is instructed when there is no connection between Dr.Web Server and the anti-virus workstation, the Agent software will be uninstalled from the selected computer once the connection is recovered.

At remote uninstallation of the Agent (uninstallation on a station is performed in the background mode), the station will be forced to restart at interval of five minutes. You cannot change the interval or cancel the restart. Station users are notified about the upcoming restart in the popup message.

Uninstalling Dr.Web Agent and Anti-Virus Package Locally

To remove the Agent and the anti-virus package locally, this option must be allowed at the Server in the **Permissions** section (see **Administrator manual**, p. Permissions of Station Users).

You can remove the station anti-virus software (Agent and anti-virus package) by the two ways:

1. By means of standard Windows OS services.
2. By using the Agent installer.

> If the Agent and anti-virus package are uninstalled via the standard Windows OS services or via the Agent installer, user will be prompt for Quarantine deleting.

Removing by Means of Standard Windows OS Services

> This removing method will be available only if you installed the Agent by using the graphical installer and set the **Register Dr.Web Agent in the system list of installed software** flag.
>
> If the Agent installed in the background mode of the installer, the removing of the anti-virus software with the standard Windows OS services will be available only if the `/regagent yes` switch was used for installation.

To remove the Agent and the anti-virus package, use standard Windows OS tools: the **Add or Remove Programs** element in **Control Panel** (see the Agent **User Manual** for details).

Removing by Using the Agent Installer

- **Client module win-es-agent-setup.exe**

  To remove the Agent software and the anti-virus package by using the client module which is created during the Agent setup, run the `win-es-agent-setup.exe` installation file with the `/instMode remove parameter`. Additionally use the `/silent no` parameter, if you want to control the process.

  The `win-es-agent-setup.exe` installation file is located in the following folder by default:

  - For Windows XP OS and Windows Server 2003 OS:
    `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`
  - For Windows Vista OS and later and Windows Server 2008 OS and later:
    `%ALLUSERSPROFILE%\Doctor Web\Setup\`

  For example, for Windows 7, where the `%ALLUSERPROFILE%` corresponds to `C:\ProgramData`:

  ```
  C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe /instMode
  remove /silent no
  ```

- **Personal installation package drweb_ess_<*OS*>_<*station*>.exe**

  To remove the Agent software and the anti-virus package by using the installation package, run the `drweb_ess_<OS>_`*<station>*`.exe` installation file of the currently installed version.

- **Full installer drweb-11.05.2-<build>-esuite-agent-full-windows.exe**

  To remove the Agent software and the anti-virus package by using the full installer, run the `drweb-11.05.2-`*<build>*`-esuite-agent-full-windows.exe` installation file of the currently installed version.

- **Network installer drwinst.exe**

  To remove the Agent software and the anti-virus package from a workstation locally by using the network installer, run in the installation folder of the Agent (by default `C:\Program Files\DrWeb`) the `drwinst.exe` installer with the `/instMode remove` parameter. Additionally use the `/silent no` parameter, if you want to control the process.

  For example:

  ```
  drwinst /instMode remove /silent no
  ```

  When you launch the `drweb_ess_`*<OS>*`_`*<station>*`.exe` installation package, the `drweb-11.05.2-`*<build>*`-esuite-agent-full-windows.exe` full installer and the `drwinst.exe` network installer, the `win-es-agent-setup.exe` client module launches and performs the removal directly.

  The `win-es-agent-setup.exe` client module launched without parameters, detects installed product and launches the change/remove mode. To launch the remove mode directly, use the `/instMode remove` switch.

5.2.2. Removing Dr.Web Agent through Active Directory

To be able to delete the Agent, this option must be allowed at the Server in the **Permissions** section (see **Administrator manual**, p. Permissions of Station Users).

1. In **Control Panel**, select **Administrative Tools** → **Active Directory users and computers**.
2. Right-click your ESS organizational unit in the domain. On the context menu, select **Properties**. An **ESS Properties** window will be opened.
3. Go to the **Group Policy** tab. Select **ESS policies**. Double-click the item. A **Group Policy Object Editor** window will be opened.
4. In the hierarchical list, select **Computer configuration** → **Software settings** → **Software installations** → **Package**. Then on the context menu, select **All tasks** → **Uninstall** → **OK.**
5. On the **Group Policy** tab, click **OK.**
6. Dr.Web Agent will be removed from the stations at the next registration in the domain.

5.3. Removing Proxy Server

The Proxy server can be uninstalled by one of the following ways:

1. Locally.

   Local deinstallation is performed by administrator directly on the computer with the Proxy server installed.
2. Remotely.

Remote deinstallation of the Proxy server is performed in the Control Center via LAN and available only if the Proxy server is connected to the Server.

5.3.1. Local Removing Proxy Server

For Windows OS

> During Proxy server uninstallation, the `drwcsd-proxy.conf` (`drwcsd-proxy.xml` for version 10 and earlier) configuration file is deleted. If necessary, save configuration file manually before Proxy server uninstallation.

The Proxy server software uninstallation is performed via the standard Windows OS tools at **Control Panel** → **Add or Remove Programs** (**Programs and components** for Windows 2008 OS and later).

For UNIX System-Based OS

> At uninstalling the Proxy server, the backup of configuration files is saved automatically to the `/var/tmp/drwcsd-proxy`.

Proxy server OS	Action
FreeBSD	Run the script: `/usr/local/etc/drweb.com/software/drweb-esuite-proxy.remove`
Linux	Run the script: `/etc/opt/drweb.com/software/drweb-proxy.remove`

5.3.2. Remote Removing Proxy Server

Remote deinstallation of the Proxy server is available when the Proxy server is connected to the Server (see Connecting the Proxy Server to Dr.Web Server).

> When deleting the Proxy server account in the Control Center, the Proxy server is uninstalled from the station.

To delete the Proxy server

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the hierarchical list of the opened window, click the name of one or several Proxy servers you want to delete.
3. On the toolbar, click ★ **General** → ✖ **Remove selected objects**.

4. You will be prompt to remove the object. Click **OK**.

To delete the Proxy server that is installed on the connected station

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. Open the station properties section by one of the following ways:
   a) Click the name of the station in the hierarchical list of the anti-virus network. A panel with properties of the station will be automatically opened in the right part of the Control Center.
   b) Click **Properties** in the control menu. A window with the station properties will be opened.
3. In the station properties window, go to the **Proxy server** section.
4. Click **Delete Proxy server**.

   After you click **Save**, the Proxy server will be deinstalled from the station. Proxy server account—deleted from the Server.

Chapter 6: Upgrading Dr.Web Enterprise Security Suite Software and Its Components

Before updating Dr.Web Enterprise Security Suite and its components, please note the following important features:

- Before updating, it is recommended to check the validity of TCP/IP protocol configuration for the Internet access. Particularly, DNS service must be enabled and properly configured.
- In multiserver anti-virus network configuration, consider that interserver updates transmission is not performed between Servers of 11 version and Servers of previous versions and interserver connection is used for transmission statistics only. To provide interserver updates transmission, you must upgrade all Servers. If you need to remain Servers of previous version as a part of the anti-virus network to connect the Agents installed on operating systems which are not supported by the 11 version (see Upgrading Dr.Web Agent), when Servers of versions 6 and Servers of the 11 version must receive updates independently.
- For the anti-virus network containing Dr.Web Proxy server, at upgrade of the components up to the version 11.0.2, you must also upgrade the Proxy server up to the version 11.0.2. Otherwise, the Agents supplied within version 11.0.2 will not be able to connect to the Server of version 11.0.2. It is recommended to perform the upgrade in the following order: Dr.Web Server → Dr.Web Proxy server → Dr.Web Agent.
- During upgrade of the Server from the 6 version to the 11 version, settings of the Sever operation via the proxy server are not saved. After the installation of the 11 version, you must specify the settings of connection via the proxy server manually (see **Administration Manual**, p. Proxy).
- At upgrading the Server, all repository settings will not be transferred to the new version (will be reset to defaults), however they are backed up. If necessary, specify the repository settings manually after the Server upgrade.

6.1. Upgrading Dr.Web Server for Windows® OS

At upgrading Dr.Web Server under Windows OS from version 10 and earlier, the settings from the following sections of the Control Center will not be transferred into the version 11:

- **Dr.Web Server configuration > Network > Download** (the `download.conf` file),
- **Dr.Web Server remote access** (the `frontdoor.conf` file),
- **Web server configuration** (the `webmin.conf` file).

Settings in these sections will be reset to defaults. If you want to use the settings of the previous version, specify them manually after the Server upgrade in the corresponding sections of the Control Center basing on the data from the configuration files backup.

Upgrading of the Server from the 6 and 10 versions to the 11 version and within version 11 is performed automatically by the means of the installer.

Before upgrading the Server, please read the Upgrading Dr.Web Agent section.

Upgrading the Server within version 11 can be also performed via the Control Center. The procedure is described in the **Administrator Manual**, in the Updating Dr.Web Server and Restoring from the Backup section.

Not all Server updates within version 11 have the distribution kit file. Some of them can be installed via the Control Center only.

Saving Configuration Files

At upgrading the Server to the 11 version by the installer means, the configuration files are saved into the folder specified for the back up:

- For the upgrade from the version 6: to the <*installation_drive*>:\DrWeb Backup.
- For the upgrade from the versions 10 and within version 11: to the folder that is specified in the **Back up Dr.Web Server critical data** option during the upgrade (<*installation_drive*>:\DrWeb Backup by default).

At upgrading of the Server of the version 6, the following files are saved:

File	Description
agent.key (name may vary)	Agent license key file
auth-ads.xml	configuration file for administrators external authorization via Active Directory
auth-ldap.xml	configuration file for administrators external authorization via LDAP
auth-radius.xml	configuration file for administrators external authorization via RADIUS
drwcsd.conf (name may vary)	Server configuration file
dbinternal.dbs	embedded database
drwcsd.pri	private encryption key
drwcsd.pub	public encryption key
enterprise.key (name may vary)	Server license key file
webmin.conf	Dr.Web Security Control Center configuration file

At upgrading of the Server of the version 10, the following files are saved:

File	Description
`agent.key` (name may vary)	Agent license key file
`auth-ads.xml`	configuration file for administrators external authorization via Active Directory
`auth-ldap.xml`	configuration file for administrators external authorization via LDAP
`auth-radius.xml`	configuration file for administrators external authorization via RADIUS
`enterprise.key` (name may vary)	Server license key file. The file is saved if it presented after the upgrade from the previous versions. For the new Server 11.0.2 installation, the file is absent
`drwcsd.conf` (name may vary)	Server configuration file
`drwcsd.conf.distr`	Server configuration file template with default parameters
`drwcsd.pri`	private encryption key
`drwcsd.pub`	public encryption key
`download.conf`	network settings for generating of the Agent installation packages
`frontdoor.conf`	configuration file for the Server remote diagnostic utility
`webmin.conf`	Control Center configuration file
`openssl.cnf`	Server certificate for HTTPS

At upgrading of the Server within version 11, the following files are saved:

File	Description
`agent.key` (name may vary)	Agent license key file
`auth-ads.conf`	configuration file for administrators external authorization via Active Directory
`auth-radius.conf`	configuration file for administrators external authorization via RADIUS
`auth-ldap.conf`	configuration file for administrators external authorization via LDAP
`auth-ldap-rfc4515.conf`	configuration file for administrators external authorization via LDAP using the simplified scheme

File	Description
auth-ldap-rfc4515-check-group.conf	configuration file template for administrators external authorization via LDAP using the simplified scheme with verification of belonging to an Active Directory group
auth-ldap-rfc4515-check-group-novar.conf	configuration file template for administrators external authorization via LDAP using the simplified scheme with verification of belonging to an Active Directory group and using variables
auth-ldap-rfc4515-simple-login.conf	configuration file template for administrators external authorization via LDAP using the simplified scheme
auth-pam.conf	configuration file for administrators external authorization via PAM
enterprise.key (name may vary)	Server license key file. The file is saved if it presented after the upgrade from the previous versions. For the new Server 11.0.2 installation, the file is absent
drwcsd-certificate.pem	Server certificate
download.conf	network settings for generating of the Agent installation packages
drwcsd.conf (name may vary)	Server configuration file
drwcsd.conf.distr	Server configuration file template with default parameters
drwcsd.pri	private encryption key
dbexport.gz	database export
drwcsd.pub	public encryption key
frontdoor.conf	configuration file for the Server remote diagnostic utility
openssl.cnf	Server certificate for HTTPS
webmin.conf	Control Center configuration file
yalocator.apikey	API key for the Yandex.Locator extension

⚠ If you are planning to use configuration files from the version 6 of the Server, please note:

1. Server license key is no longer supported (see Chapter 2: Licensing).
2. The embedded database is upgraded and configuration files of the Server is converted by the means of the installer. You cannot replace these files with a backup copies when upgrading from the Server of version 6.

If necessary, copy other critical files you want to preserve to another folder, other than Server installation folder. For instance, report templates which are stored in the `\var\templates` folder.

Saving Database

> The MS SQL CE database starting from the 10 version of Dr.Web Server is no longer supported. During automatic Server upgrade by the means of the installer, the MS SQL CE database is automatically converted to the `SQLite` embedded database.

Before upgrade Dr.Web Enterprise Security Suite software, it is recommended to backup database.

To backup database

1. Stop the Server.
2. Export the database to the file:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all exportdb <backup_folder>\esbase.es
```

For Servers with external database, it is recommended to use standard tools supplied with the database.

> Make sure, that Dr.Web Enterprise Security Suite database export completed successfully. If the database backup copy is not available, the Server could not be restored in emergency case.

Upgrading Dr.Web Server

To upgrade Dr.Web Server, run the distribution file.

> By default, installer uses the language of the operating system. If necessary, you can change the installation language on any step by selecting the corresponding option in the right upper part of the installer window.
>
> For the external Server database, also select **Use existing database** during upgrade.

> If you are going to use the Oracle DB as an external database via the ODBC connection, then during installation (upgrading) of the Server, in the installer settings, disable the installation of embedded client for Oracle DBMS (in the **Database support → Oracle database driver** section).
>
> Otherwise, interaction with the Oracle DB via ODBC will fail because of the libraries conflict.

Upgrade from the Version 6

1. The window opens, which notifies you on the previous Dr.Web Server version installed and brief description of the upgrade process to a new version. To start configuring upgrade procedure, click **Upgrade**.
2. The next window contains the information on the product and the link to the license agreement text. When you read the agreement, to continue the installation, select **I accept the terms of the license agreement** and click **Next**.
3. On the following steps, the upgrading Server is configured as at the Installing Dr.Web Server process based on the configuration files from the previous installation. The installation wizard automatically locates the Server installation folder, configuration files and embedded DB location from the previous installation. If necessary, you can change locations of the files which were found automatically by the installer.
4. To uninstall the Server of the previous version and launch the installation process of the 11.0.2 version of the Server, click **Install**.

   During the Server uninstallation, the configuration files are automatically saved to the *<installation_drive>*`:\DrWeb Backup` folder.

Upgrade from the Version 10.0

1. The window opens, which notifies you on the previous Dr.Web Server version installed and brief description of the upgrade process to a new version. To start configuring upgrade procedure, click **Upgrade**.
2. The next window contains the information on the product and the link to the license agreement text. When you read the agreement, to continue the installation, select **I accept the terms of the license agreement** and click **Next**.
3. On the following steps, the upgrading Server is configured as at the Installing Dr.Web Server process based on the configuration files from the previous installation. The installation wizard automatically locates the Server installation folder, configuration files and embedded DB location from the previous installation. If necessary, you can change locations of the files which were found automatically by the installer.
4. To uninstall the Server of the previous version and launch the installation process of the 11.0.2 version of the Server, click **Install**.
5. During the update, the window opens that contains the critical data backup settings before uninstalling the Server of the previous version. It is recommended to set the **Back up Dr.Web Server critical data** flag. If necessary, you can change the default backup folder (*<installation_drive>*`:\DrWeb Backup`).

Upgrade from the Versions 10.0.1, 10.1 and within version 11

1. The window opens, which notifies you on the previous Dr.Web Server version installed and brief description of the upgrade process to a new version. To start configuring upgrade procedure, click **Upgrade**.

2. The next window contains the critical data backup settings before uninstalling the Server of the previous version. It is recommended to set the **Back up Dr.Web Server critical data** flag. If necessary, you can change the default backup folder (<*installation_drive*>`:\DrWeb Backup`). Click **Uninstall** to start the uninstalling of the Server of previous version.
3. After the previous version is uninstalled, the new version of the Server starts the installation. The next window contains the information on the product and the link to the license agreement text. When you read the agreement, to continue the installation, select **I accept the terms of the license agreement** and click **Next**.
4. On the following steps, the upgrading Server is configured as at the Installing Dr.Web Server process based on the configuration files from the previous installation. The installation wizard automatically locates the Server installation folder, configuration files and embedded DB location from the previous installation. If necessary, you can change locations of the files which were found automatically by the installer.
5. To start the installation of the Server of version 11.0.2, click **Install**.

> ⚠ After upgrade of anti-virus network Servers is completed, you must do the following:
>
> 1. Configure encryption and compression settings for the connected Servers (see the **Administrator Manual**, the Setting Connections between Several Dr.Web Servers section).
> 2. Clear the cache of the Web browser that is used to connect to Dr.Web Security Control Center.

6.2. Upgrading Dr.Web Server for UNIX® System-Based OS

> ⚠ At upgrading Dr.Web Server under UNIX system-based OS from version 10 and earlier, the settings from the **Web server configuration** (the `webmin.conf` file) section of the Control Center will not be transferred into the version 11.
>
> Settings in this section will be reset to defaults. If you want to use the settings of the previous version, specify them manually after the Server upgrade in the corresponding section of the Control Center basing on the data from the configuration file backup.
>
> ---
>
> All actions must be performed under the **root** administrator account.

Upgrade of the Server up to the version 11 depends on the initial version:

- Upgrade from the version 6.0.4 to the version 11 can be made only manually.
- Upgrade from the version 10 to the version 11 automatically over the installed version is possible not for all UNIX system-based OS. Thus, under UNIX system-based OS, on which automatic upgrading over the installed package is not supported, you must perform the upgrade manually.
- Upgrading the Server software within version 11 for the same package types is performed automatically for all UNIX system-based OS. If needed, you can also perform the upgrade manually.

Before removing the Server of previous version, please read the Upgrading Dr.Web Agent section.

Upgrading the Server within version 11 can be also performed via the Control Center. The procedure is described in the **Administrator Manual**, in the Updating Dr.Web Server and Restoring from the Backup section.

Not all Server updates within version 11 have the distribution kit file. Some of them can be installed via the Control Center only.

Saving Configuration Files

At uninstalling and automatic upgrading of the Server to the version 11, configuration files are saved into default backup directory : `/var/tmp/drwcs/`.

After the Server of 6 version has been removed, the following files are automatically saved:

File	**Description**
`agent.key` (the name may vary)	Agent license key file
`certificate.pem`	SSL certificate
`common.conf`	configuration file (for some UNIX system-based OS)
`dbinternal.dbs`	embedded database
`drwcsd.conf` (the name may vary)	Server configuration file
`drwcsd.pri`	private encryption key
`drwcsd.pub`	public encryption key
`enterprise.key` (the name may vary)	Server license key file
`private-key.pem`	RSA private key
`webmin.conf`	Dr.Web Security Control Center configuration file

After the Server of 10 version has been removed, the following files are automatically saved:

File	**Description**
`agent.key` (the name may vary)	Agent license key file

File	Description
auth-ldap.xml	configuration file for administrators external authorization via LDAP
auth-pam.xml	configuration file for administrators external authorization via PAM
auth-radius.xml	configuration file for administrators external authorization via RADIUS
certificate.pem	SSL certificate
common.conf	configuration file (for some UNIX system-based OS)
dbexport.gz	database export (created during the Server uninstallation using the command drwcs.sh xmlexportdb)
download.conf	network settings for generating of the Agent installation packages
drwcsd.conf (the name may vary)	Server configuration file
drwcsd.pri	private encryption key
drwcsd.pub	public encryption key
enterprise.key (the name may vary)	Server license key file. The file is saved if it presented after the upgrade from the previous versions. For the new Server 11.0.2 installation, the file is absent
frontdoor.conf	configuration file for the Server remote diagnostic utility
local.conf	Server log settings
private-key.pem	RSA private key
webmin.conf	Dr.Web Security Control Center configuration file
*.dbs *.sqlite	embedded database

After the Server of 11 version has been removed, the following configuration files are automatically saved:

File	Description
agent.key (the name may vary)	Agent license key file
auth-ldap.conf	configuration file for administrators external authorization via LDAP

File	Description
`auth-ldap-rfc4515.conf`	configuration file for administrators external authorization via LDAP using the simplified scheme
`auth-pam.conf`	configuration file for administrators external authorization via PAM
`auth-radius.conf`	configuration file for administrators external authorization via RADIUS
`certificate.pem`	SSL certificate
`common.conf`	configuration file (for some UNIX system-based OS)
`dbexport.gz`	database export (created during the Server uninstallation using the command `drwcs.sh xmlexportdb`)
`download.conf`	network settings for generating of the Agent installation packages
`drwcsd-certificate.pem`	Server certificate
`drwcsd.conf` (the name may vary)	Server configuration file
`drwcsd.pri`	private encryption key
`drwcsd.pub`	public encryption key
`enterprise.key` (the name may vary)	Server license key file. The file is saved if it presented after the upgrade from the previous versions. For the new Server 11.0.2 installation, the file is absent
`frontdoor.conf`	configuration file for the Server remote diagnostic utility
`local.conf`	Server log settings
`private-key.pem`	RSA private key
`webmin.conf`	Dr.Web Security Control Center configuration file
`yalocator.apikey`	API key for the Yandex.Locator extension

After the automatic upgrade, the following files are saved to the backup directory:

For the Server version 10:

File	Description
`auth-ldap.xml`	configuration file for administrators external authorization via LDAP
`auth-pam.xml`	configuration file for administrators external authorization via PAM

File	Description
`auth-radius.xml`	configuration file for administrators external authorization via RADIUS
`db.backup.gz`	database export (created during the Server upgrade using the command `drwcs.sh exportdb`)

For the Server version 11:

File	Description
`auth-ldap.conf`	configuration file for administrators external authorization via LDAP
`auth-ldap-rfc4515.conf`	configuration file for administrators external authorization via LDAP using the simplified scheme
`auth-pam.conf`	configuration file for administrators external authorization via PAM
`auth-radius.conf`	configuration file for administrators external authorization via RADIUS
`db.backup.gz`	database export (created during the Server upgrade using the command `drwcs.sh exportdb`)

If you are planning to use configuration files from the version 6 of the Server, please note:

1. Server license key is no longer supported (see Chapter 2: Licensing).
2. The embedded database is upgraded and configuration files of the Server is converted by the means of the installer. You cannot replace these files with a backup copies when upgrading from the Server of version 6.

Saving Database

Before upgrade Dr.Web Enterprise Security Suite software, it is recommended to backup database.

To backup database

1. Stop the Server.
2. Export DB to the file:
   - For FreeBSD OS:
     ```
     # /usr/local/etc/rc.d/drwcsd exportdb /var/tmp/esbase.es
     ```
   - For Linux OS:
     ```
     # /etc/init.d/drwcsd exportdb /var/tmp/esbase.es
     ```

For Servers with external DB, it is recommended to use standard tools supplied with the database.

Make sure, that Dr.Web Enterprise Security Suite DB export completed successfully. If DB backup copy is not available, the Server could not be restored in emergency case.

Automatic Upgrade

If you upgrade the Server from 10 version to version 11 (except the Servers installed under **Linux** OS from the `*.rpm.run` and `*.deb.run` packages), instead of deleting the old version and installing the new version of the Server, you can use the package upgrade. For this, launch the installation of corresponding Server package.

Upgrading the Server software within version 11 for the same package types is performed automatically for all UNIX system-based OS.

At this, configuration files will be automatically converted and placed in corresponding directories. Also, some configuration files are additionally stored in the backup directory.

Manual Upgrade

If the Server upgrade from the version 6.0.4 and later cannot be done over the installed package, you must delete the Server software of previous versions saving the backup copy and install the software of the version 11 based on the saved backup copy.

To upgrade Dr.Web Server perform the following procedure:

1. Stop the Server.
2. If you plan to use any files (besides the files which are copied automatically during the Server uninstall at step **3**), backup these files manually, for example, the report templates and etc.
3. Remove the Server software (see Removing Dr.Web Server Software for UNIX® System-Based OS). You will be prompt to create a backup copies of the files. For this, specify the path to store the backup or accept the default path.
4. Install Dr.Web Server version 11.0.2 according to the general installation procedure (see Installing Dr.Web Server for UNIX® System-Based OS) based on the backup copy from the step **3**. All saved configuration files and embedded database (if you use embedded database) will be automatically converted to be used by the Server of the 11.0.2 version. Without automatic conversion, database (if you use embedded database) and some of the Server configuration files from the previous version cannot be used.

   In case of manual backup, place the files to the same directories where they were located in the previous version.

For all backup files from the previous Server version (see step 4) you must set the user selected at the installation of the new Server version (**drwcs** by default), as files owner.

5. Launch the Server.
6. Set up repository upgrade and perform the upgrade.

> ⚠ After upgrade of anti-virus network Servers is completed, you must configure encryption and compression settings for the connected Servers (see the **Administrator Manual**, the Setting Connections between Several Dr.Web Servers section).

6.3. Upgrading Dr.Web Agent

The Agent upgrade after the Server upgrade is described for the following variants:

1. Upgrading Dr.Web Agents on Stations under Windows® OS,
2. Upgrading Dr.Web Agents on Stations under Android OS,
3. Upgrading Dr.Web Agents on Stations under Linux® and macOS®.

6.3.1. Upgrading Dr.Web Agents on Stations under Windows® OS

Upgrade of the Agents Supplied with Dr.Web Enterprise Security Suite 10

Upgrade of the Agents supplied with Dr.Web Enterprise Security Suite 10 is performed automatically.

After the automatic upgrade, the popup notification with restart request is displayed on a station; in the Control Center, restart request after the upgrade is displayed in the station status. Restart a station locally or remotely via the Control Center to complete the upgrade.

If the station was connected to the Server via the Dr.Web Proxy server of version 10 and earlier, you must upgrade the Proxy server up to the version 11 or remove the Proxy server before the Agent upgrading.

Automatic Upgrade of the Agents Supplied with Dr.Web Enterprise Security Suite 6

To perform automatic upgrade, the following conditions must be met:

1. Agents must be installed on a computers under Windows OS which are supported for the installation of Agents for Dr.Web Enterprise Security Suite version 11.0.2 (see the **Appendices** document, Appendix A. The Complete List of Supported OS Versions).
2. For the automatic upgrade, the following actions are possible depending on the Server settings:

a) Automatic upgrade is performed, if during the Server upgrade, encryption keys and network settings from the previous Server were saved.

b) The manual configuration required during the automatic upgrade, if during the Server upgrade, new encryption keys and Server network settings were specified.

> Please note the following features during automatic upgrade:
>
> 1. After removing the Agent, notification on reboot required is not displayed on a station. Administrator must initiate the station reboot.
> 2. Between the removal of an old Agent version and installing of a new version, stations will have no anti-virus protection.
> 3. After upgrading of the Agent, the anti-virus software operation will be limited without the station restart. At this, the complete anti-virus protection of the station is not provided. User must restart the station on the Agent demand.

Automatic upgrade of the Agent is performed by the following procedure:

1. The old version of the Agent is uninstalled when upgrade is started.
2. The station is rebooted manually.
3. The new version of the Agent is installed. For this, the task in the Server schedule is automatically created.
4. After the Agent upgrade is completed, the station automatically connects to the Server. In the **Status** section of the Control Center, the notification on required restart will be displayed for the upgraded station. The station must be restarted.

Automatic upgrade of the Agent with manual configuring is performed by the following procedure:

1. Configure settings for connection to the new Server and replace public encryption key on station manually.
2. After changing of the settings on the station and connecting the stations to the Server, the Agent upgrade process starts.
3. The old version of the Agent is uninstalled when upgrade is started.
4. The station is rebooted manually.
5. The new version of the Agent is installed. For this, the task in the Server schedule is automatically created.
6. After the Agent upgrade is completed, the station automatically connects to the Server. In the **Status** section of the Control Center, the notification on required restart will be displayed for the upgraded station. The station must be restarted.

Manual Upgrade of the Agents Supplied with Dr.Web Enterprise Security Suite 6

If installation of the new version of the Agent during automatic upgrade failed for any reason, the next installation attempts are not performed. No anti-virus software will be installed on the station, and such station will be displayed as offline in the Control Center.

In such case, you must install the Agent by yourself. At this, after the new Agent installation, you must merge the new station and the old station in the Control Center, in the hierarchical tree of the anti-virus network.

Upgrade is not Supported

If Agents are installed on stations under OS which are not supported for the installation of Agents for Dr.Web Enterprise Security Suite version 11.0.2, actions to upgrade are not performed.

Agents installed on unsupported OS cannot receive updates (including virus bases updates) from the new Server. If you need to remain Agents under unsupported OS, you must leave the Server of previous version to which these Agents are connected as a part of the anti-virus network. At this, Servers of 6 versions and Servers of the 11.0.2 version must receive updates independently.

> Recommendations on upgrading the Agents, installed at the stations that implement significant LAN functions, specified in the **Appendices** document, p. Upgrading Dr.Web Agents on the LAN servers.

6.3.2. Upgrading Dr.Web Agents on Stations under Android OS

> Dr.Web Agents for Android must be upgraded manually on mobile devices to operate with Dr.Web Enterprise Security Suite of version 11.0.2.
>
> ---
>
> Dr.Web Enterprise Security Suite of version 11.0.2 supports only Dr.Web Agents for Android of version 12.2 and later.
>
> At regular upgrade of Dr.Web Agents for Android, mobile devices protection will be disabled due to the error of incompatible virus databases version.

To upgrade Dr.Web Agents for Android locally, you can use one of the following ways:

1. If you can download separately the installation package of the Agent standalone version via the Internet.

Before upgrading Dr.Web Server, upgrade Dr.Web Agents for Android manually on mobile devices up to the version 12.2 or later. You can download the new version on Doctor Web company web site at https://download.drweb.com/android/. The new Agent will connect to the Server of previous version normally, after that you can upgrade the Server up to the version 11.0.2 according to the general procedure.

2. If you cannot download separately the installation package of the Agent standalone version via the Internet.

   After upgrade of Dr.Web Server, Dr.Web Agents for Android will automatically connect to the upgraded Server. After the upgrade attempt, the protection will be disabled on mobile devices due to the error of incompatible virus databases version. Upgrade the Agents manually directly on mobile devices. You can download installation package of the Agent new version in the Control Center, in the station properties or on the installation page.

3. If you cannot download separately the installation package of the Agent standalone version via the Internet, and the upgrade error occurrence on a mobile device is unwanted.

   Before upgrading the Server, disconnect Dr.Web Agents for Android. In this case, mobile devices will not be able to connect to the new Server for downloading incompatible updates. Upgrade the Server up to the version 11.0.2 according to the general procedure. Download installation package of the Agent new version in the Control Center, in the station properties or on the installation page. Upgrade the Agents manually on mobile devices. Connect upgraded Agents to the new Server.

6.3.3. Upgrading Dr.Web Agents on Stations under Linux® and macOS®

Agents installed on stations under Linux system-based OS and macOS connect to the Server of the 11.0.2 version if the following conditions are met:

1. Agents must be installed on a computers under operation systems which are supported for the installation of Agents for Dr.Web Enterprise Security Suite version 11.0.2 (see the **Appendices** document, Appendix A. The Complete List of Supported OS Versions).
2. Encryption keys and network settings from the upgraded Server must be set on the stations.

After connecting the stations to the updated Server:

1. Only virus databases will be updated on stations. Automatic upgrade of the anti-virus software itself is not performed.
2. If the last software version is installed on stations, no actions required.
3. If the software on stations is outdated, download installation package of the Agent new version in the Control Center, in the station properties or on the installation page. Upgrade the station software manually as described in the corresponding **User Manual**.

6.4. Upgrading Dr.Web Proxy Server

6.4.1. Updating Dr.Web Proxy Server During Operation

The Proxy server can be updated automatically during its operation.

Updates schedule depends on the settings of the Proxy server proactive caching:

1. If the Proxy server is not included into the list for the proactive caching (including if the caching is not used), when the Proxy server updates will be downloaded and installed according to the automatic updates schedule.
2. If the Proxy server is included into the list for the proactive caching, the Proxy server updates will be automatically downloaded according to the proactive caching schedule. When a new revision of the Proxy server is received, the update to this revision is performed according to the automatic updates schedule.

You can configure the automatic updates by one of the following ways:

- Via the Proxy server settings in the Control Center of the managing Server, in the **Updates** section. Detailed description is given in the **Administrator Manual**, in the Remote Configuration of the Proxy Server section.
- Via the Proxy server configuration file `drwcsd-proxy.conf`. Detailed description is given in the **Appendices** document, p. Appendix G4.

6.4.2. Updating Dr.Web Proxy Server via the Installer

Proxy Server Configuration Files

Configuration file of the Proxy server of version 10 and earlier:

File	Description
`drwcsd-proxy.xml`	Proxy server configuration file (see the **Appendices** document, p. Appendix G4)

Configuration files of the Proxy server of version 11 and later:

File	Description
`drwcsd-proxy.conf`	Proxy server configuration file (see the **Appendices** document, p. Appendix G4)
`drwcsd-proxy.auth`	credentials (ID and password) to access Dr.Web Servers

File	Description
`drwcsd-proxy-trusted.list`	list of trusted certificates of Dr.Web Servers
`drwcsd-proxy-signed.list`	list of signed certificates of the Proxy server
`drwcsd-proxy.pri`	private encryption key of the Proxy server

Upgrading Proxy Server under Windows OS

Upgrade of the Proxy server is performed automatically by the means of the installer.

To upgrade Proxy server of version 10 and earlier

1. Run the Proxy server distribution file.
2. The opened window notifies you on the previous Proxy server version installed and invites to upgrade to a new version. To start uninstalling of previous version and installing the new version, click **Upgrade**.
3. The next window contains the information on the product. Click **Next**.
4. On the following steps, the upgrading Proxy server is configured as at the Installing Dr.Web Proxy server process based on the configuration file from the previous installation. The installation wizard automatically locates the Proxy server installation folder and configuration file from the previous installation. If necessary, you can change settings from the file which was found automatically by the installer.
5. To start the installation of the Proxy server of version 11.0.2, click **Install**.

To upgrade Proxy server from version 11 and later

1. Run the Proxy server distribution file.
2. The opened window notifies you on the previous Proxy server version installed and invites to upgrade to a new version. To start configuring upgrade procedure, click **Upgrade**.
3. The next window contains the information on uninstalling of the previous version of the Proxy server. Click **Uninstall** to start the uninstalling process.
4. After the previous version of the Proxy server is uninstalled, a new version starts the installation. The next window contains the information on the product. Click **Next**.
5. On the following steps, the upgrading Proxy server is configured as at the Installing Dr.Web Proxy server process based on the configuration files from the previous installation. The installation wizard automatically locates the Proxy server installation folder and configuration files from the previous installation. If necessary, you can change settings from the files that were found automatically by the installer.
6. To start the installation of the Proxy server of version 11.0.2, click **Install**.

Upgrading Proxy Server under UNIX System-Based OS

To upgrade Proxy server of version 11.0 and earlier

> ⚠ During Proxy server upgrading, the configuration files are deleted. If necessary, save configuration files manually before the upgrading.

1. To start the upgrade process, run the Proxy server distribution file:
   `./`*<distribution_file>*`.tar.gz.run`
2. If necessary, manually transfer the settings from the configuration files saved before the upgrade process to the new configuration files.

To upgrade Proxy server from version 11.0.1

1. To start the upgrade process, run the Proxy server distribution file:
   `./`*<distribution_file>*`.tar.gz.run`
2. During the uninstallation of the previous version, the configuration files of the Proxy server will be automatically saved.
3. During the upgrade, you will be prompted to use configuration files from a previous Proxy server installation, saved during the backup:
   - To use the default backup saved in `/var/tmp/drwcsd-proxy`, press ENTER.
   - To use the backup from the other directory, specify the path to the backup manually.
   - Also, you can install the Proxy server with the default settings not using the backup configuration from the previous version. For this, press 0.

Keyword Index

Keyword Index